

ALAGAPPA UNIVERSITY

(Reaccredited with 'A' Grade by NAAC)
Karaikudi - 630 003, TAMILNADU



DIRECTORATE OF DISTANCE EDUCATION

(Recognized by Distance Education Council (DEC), New Delhi)

M.B.A

(Project Management)



Paper 4.1

Project Risk Management

ALAGAPPA UNIVERSITY

KARAIKUDI - 630 003 TAMILNADU

DIRECTORATE OF DISTANCE EDUCATION

M.B.A. (Project Management)

(III Semester)



Paper 4.1

PROJECT RISK MANAGEMENT

AU/DDE/D2/Printing/Order 6/2015 Date: 17-02-15 500 Copies
POWERMAN PRINTERS, CHENNAI -21. Cell No. 9840823160

Paper 4.1 PROJECT RISK MANAGEMENT

UNIT 1

Risk Management: Concept and objectives – Definition of risk and uncertainty – Classification of risk: Pure and speculative risks – Cost of risk – Risk management process – Contributions of risk management to business, society and family.

UNIT 2

Risk Management in Business: Risk vis-à-vis size and types of business – Scope of risk manager's duties – Risk management corporate policy and strategy.

UNIT 3

Risk Identification and Measurement: Identification methods: Checklist, questionnaire, financial statement analysis, flow-chart, on-site inspection, record of losses, threat analysis, event analysis, safety audit – Measurement methods: Frequency and severity measures – Probability approach.

UNIT 4

Risk Exposure Losses: Property loss exposures – Types – Net income loss exposures – Valuation of potential loss – Decrease in income – Increase in expenses – Liability loss exposure: Civil liabilities of business houses: Form contracts, omissions, commissions, bankruptcy, etc.

UNIT 5

Risk Management Techniques: Avoidance – Loss control – Separation – Combination – Transfer.

Risk Retention: Concept and need – Methods of financing risk retention – Insurance – Reinsurance.

UNIT 6

Approaches to selecting risk management tools: Quantitative approaches: Loss method – Expected loss method – Worry method – Critical probability method – Risk adjusted capital budgeting.

REFERENCES :

1. ArthurWilliams C,Richard M Heins,*Risk Management and Insurance*,McGraw Hill.
2. Ahearn J L and Pritehett S T, *Risk Insurance*, West Publishing Co.
3. Lalley P Edward, *Corporate Uncertainty and Risk Management*, New York Risk Management Society Publication.
4. *Insurance Institute of India: Study Materials.*

Course Material Prepared by –

M.SIVAKUMAR

Lecturer in Management Studies

PSNA College of Engg & Tech., Dindigul -624 622.

UNIT 1

RISK MANAGEMENT

Risk management is a structured form of risk control that unearths possible problems early on, and thus ensures that the project will be better managed. The risk management is defined as follows:

"The entire set of activities and measures that are aimed at dealing with risks in order to maintain control over a project".

Risk Management can help to:

- Promote an uninterrupted progression of the activities with in a project and, by implementing the appropriate measures, remove any interruptions as quickly as possible should they occur;
- Instill confidence in the project, in third parties, and in the project team itself;
- Promote communication with in the project;
- Support the decision –making process with in a project.

Risk management is a cyclical process that must be repeated regularly during the course of a project. Risk management begins with the analysis of risk.

Risk management is not a new concept. It has been used in major corporations for many years. There is not a major corporation worth its salt that does not perform some sort of risk management. In general terms, risk management is a generic system that can be applied to any situation no matter how large or small. Risk management is the process of identifying, assessing and controlling or minimizing a certain risk that may involve bodily harm or financial loss.

Risk management has become more critical in the 1990's and will without any doubt be with us into the millennium. Risk management is not an isolated function of a standing committee of some association or company that

does not have the direct involvement of the people most affected. It requires involvement, commitment and a desire to achieve without excuses. When any activity is planned or envisioned the individuals in charge must list the potential risks, as well as assess them.

In the risk management context this usually leads more toward crisis management. Crisis management tends to deal as issues arise and provide short term results. Effective risk management must consider the long-term results so as to provide the required foundation for changes in activities, attitudes, objectives and situations.

Introduction to Project Risk Management

Managing risk is one of the major processes of Corporate Governance and all its aspects. Risk management is a core discipline that assists managers at all levels to make correct and informed decisions. Risk management is a process for organized assessment and control of risks. It involves the identification, analysis and evaluation of the risks presented by the system being acquired and the activities to acquire it, and the development of cost-effective treatments for those risks. It applies to projects and programs of all sizes.

Risk management is one of the seven project processes identified by international standard ISO/IEC 15288:2002 Systems engineering – System life cycle processes. The other six processes are:

- Project Planning
- Project Assessment
- Project Control
- Decision Making
- Configuration Management and
- Information Management.

In addition enterprise processes include: Investment Management, Life-cycle Processes Management, Resource Management and Quality Management. ISO 15288 provides the framework for current leading practice and failure to implement these processes is a risk that will jeopardize a project.

Risk management can be challenging because it requires thinking that may be seen as detrimental to a project. Good risk identification requires 'negative thinking' and looking for potential problems. This can be seen as at odds with the 'can-do' attitude often expected by senior management. However, looking for difficulties and then managing them so that there are 'no surprises' for senior management leads to successful projects and is a mark of mature governance. Ignoring risks or being ignorant of them leads to failure.

Effective risk management has costs. However, one recent study indicated that effective risk management could provide up to a 20:1 return on investment. It is an overhead to prevent loss.

Risk management is a tool which, with in the framework of the project based approach, can play a supporting role in gaining better control over a project. A number of control aspects are encapsulated in the concept of the project-based approach: Time, Money, Quality, Information and Organization. Control over the project may be exercised with these five factors.

Concept and Objectives

Risk management involves the identification, analysis and evaluation of a project's risks and the development of cost effective strategies to treat those risks. The management of risks is one of three core elements of a project, alongside Change Management and Quality Management, each the subject of separate Office of Information and Communications Technology (OICT) guidelines.

Concepts

Risk management is more than just the management of project risks, it is also the management of the risks that the project may place on the business. For example, if a project replaces a key system that supports services to an agency's clients then non-delivery, or provision of a system that is difficult to use, could severely degrade the agency's operations and service delivery capabilities.

Risk management is an iterative process for identifying, analyzing, evaluating, treating and monitoring risks. It is governed by a Risk Management Plan and controlled via a Risk Register.

Effective risk management requires an investment of resources. Furthermore, risk management for a particular project cannot be efficiently addressed without an organizational context to provide policies and guidance. Therefore, a key goal for risk management is to cultivate support among those who do not have a direct business interest in the actions and resources needed to treat risks. Good governance requires an organization to have documented and approved policies for risk management.

Risks are significant uncertainties about outcomes, the uncertainty is in two dimensions, the likelihood of the risk event occurring, and the extent of the consequences if it does. Different domains use different terms for risks. For example security tends to use 'threat' while occupational health and safety (OH&S) or environment uses 'hazard'. For projects it is usually convenient to refer to 'risk events'. Whatever term is used it is always important to understand the sources of the risk event.

Risk events give rise to problems, some of which may be absorbed or accommodated, but others have impacts that affect project objectives. Naturally, there is seldom a one to one relationship.

The consequences of an uncertainty can be negative or positive. While it is usual to focus on the negative risks, positive risks cause opportunities not problems. Consideration of possible positive consequences enables projects to exploit them beneficially.

If a risk event occurs before it is treated then it is a problem that changes the current reality. It then has to be managed via treatments to reduce its impact or contingency plans, or new plans if it was unforeseen. An undesirable event that is a certainty in terms of its likelihood and consequences is also a problem, not a risk. It has to be managed as part of the normal project planning or re-planning process. An issue is not necessarily a risk, it is a 'point of debate, discussion or dispute that requires resolution'. An issue may be either an uncertainty, its resolution means treating it as a risk, or a certainty in which case it is a problem to be actioned.

However, while a problem may be certain all its ramifications may be unclear. Risk management techniques may be applicable in selecting the optimum solution to the problem. This highlights the important role of risk management techniques in system engineering.

The risks associated with a project can be:

- Inherent, which result from the nature of the project objectives and scope;
- Acquired, which result from the selected organization, approach, technology, methods, tools, techniques, skills and experience that are applied to the project; or
- Contextual, which result from events, circumstances or inter-relationships outside or across the project or system boundary and impact aspects of the project.

Inherent risks are more difficult to reduce but can be managed, often through a change in the nature or scope of the project. For example, a project may have a high implementation risk due to the wide scope of the new system. Breaking the project into increments that deliver successively more operational capacity may significantly reduce this risk, providing the system level architectural design is right. And this proviso is, of course, an acquired risk.

It is normally neither feasible nor necessary to eliminate all the risks associated with a project. However, once they are identified and documented the risks can be cost effectively treated.

Effective management of risk will usually require a balance to be struck between the:

- Scope and quality of the project's deliverables and the extent to which they satisfy the needs of the business;
- Time-scale for the project;
- Cost of the project.

Effective management of project risks requires:

1. **Commitment at all levels**

The commitment to managing a project's risks must start with the agency's senior management and Sponsor and continue through all participants and stakeholders in the project.

2. **Communication and consultation**

The project must maintain contact with their internal and external stakeholders at every stage of the risk management process and concerning the process as a whole. Risks are prone to varying perceptions and it is important to reflect and reconcile these.

3. **Effective system engineering and project management**

The project must ensure that there are plans and processes for managing the project's risks. The project's management team should, through participation in similar projects, have a good understanding of the risks that the project may face and of appropriate methods for managing those risks.

4. **Risk ownership**

Each identified risk must be assigned to the person, role, team, unit or agency best able to manage it in terms of their responsibilities. They must have the overall responsibility and authority for managing the risk.

5. **A continuous approach**

Risk management is a continuous process throughout all stages of a project. The project team must constantly monitor the project's risks to assess the effectiveness of the risk management measures, to identify any new or changing risks, and develop revised risk treatments as appropriate.

6. **A partnership approach**

The project stakeholders, including project team (both in-house and contractor), the business and contextual influencers such as related projects must work closely together to identify and manage risks.

7. **An appropriate risk management process**

The use of proven methods can significantly increase the effectiveness of the risk management process. Appropriate methods and techniques, used by experienced managers and team members, will guide the identification and analysis of risks and will assist with the development of effective risk treatments.

Objectives of Project Risk Management:

The objective of project risk management is to apply a systematic process to reduce cost-effectively the effects of uncertainties that compromise project or business objectives.

All projects have risks and cost-effective management of risk is essential if a project is to achieve its business outcomes. These typically include cost, schedule, quality and the fulfillment of functional and non-functional requirements. Risk management starts at the inception of a project. This means risk must be addressed when the project's scope and justification are documented in its business need proposal and in its initial Business.

The scope of risks in projects is broad, and provides checklists of matters that should be considered. The risks are not limited to matters in the life of the project to deliver a system to the project's customer. They include risks affecting the delivered system's operational life. These impact the system design and must be managed as part of the system engineering process.

Roles of Risk Management

The key roles in risk management, and their major responsibilities are:

Senior management, who must promulgate organizational risk management policy, actively support the risk management actions required for the project and ensure that all project stakeholders and participants support those actions. The extent of their routine involvement in a particular project will depend on the project's characteristics.

Sponsor, is responsible for:

- Ensuring that adequate resources are available to manage the project's risks;
- Ensuring there is active participation in the risk management process by a wide cross section of stakeholders in the project;
- Ensuring that risks that affect the project from outside the project boundary are managed;

- Monitoring and reporting the progress and effectiveness of the risk treatments.

Project Manager / Director, heads the project team and is assigned the authority and responsibility for meeting the project objectives including the overall management of risks within the project.

Risk Owners,_who have the overall responsibility and authority for treating the identified risks. Within the project team they would be work package managers but risks to the in-service system may belong to the business unit owning the system. Risk owners must have the resources necessary to treat their risks. Risk owners are also assigned to monitor risks that are not being treated.

Risk Manager, the person in the project with the overall responsibility, accountability and authority for ensuring that the risk management process is applied effectively, including:

- Driving and managing all aspects of the risk management process;
- Developing and maintaining the Risk Management Plan,
- Ensuring all risks have an appropriate owner;
- Maintaining the Risk Register,
- Ensuring appropriately frequent risk reviews to identify new or changing risks;
- Continually monitoring the cost-effectiveness and practicability of the risk treatments;
- Preparation of regular risk reports in accordance with the Risk Management Plan; and
- Seeking and implementing continuous improvement to the risk management process and sharing lessons with other projects and stakeholders.

Business representatives and Business Owner, who must assist with the identification, analysis and evaluation of risks and support the implementation of the selected risk treatments.

Project team members, who are responsible for:

- Assisting with the identification, analysis and evaluation of risks
- Assisting with the development of risk treatments; and
- Risk management activities as set out in the risk treatments.

Definition of Risk and Uncertainty

Risk is exposure to uncertainty. Thus, risk has two components: Uncertainty and Exposure to that uncertainty. For example, if a man jumps out of an airplane with a parachute on his back, he may be uncertain as to whether or not the chute will open. He is taking a risk because he is exposed to that uncertainty. If the chute fails to open, he will suffer personally. In this example, a typical spectator on the ground would not be taking risk. They may be equally uncertain as to whether the chute will open, but they have no personal exposure to that uncertainty. Exceptions might include:

- A spectator to whom the man jumping from the plane owes money
- A spectator who is a member of the man's family
- Such spectators do face risk because they may suffer financially and/or emotionally should the man's chute fail to open they are exposed to the uncertainty.
- The financial services industry is primarily concerned with financial risk which is financial exposure to uncertainty

Classification of Risk

There have been many different attempts to classify risks, from the simple to the extremely complex. At the simple end of the spectrum is the basic breakdown of banking risk into credit risk, market risk and operational risk. More complex classification systems are intended for use as the basis of Enterprise Risk Management or other comprehensive risk management exercises.

The rationale for attempting to classify risks is that in order to manage your risks effectively you have to know what they are, and a risk classification

system is necessary in order to do this. It can provide a basis for both identification and control, two essential parts of the risk management process.

Pure and Speculative Risk

Businesses also face risks beyond these market and economic shifts. For example, a merchandise shipment of tennis shoes may be destroyed in transit. A warehouse may burn down and large amounts of expensive inventory may be lost. Events like these threaten the security of a business. They cost money, and they may cause a business to fail. First, entrepreneurs must be able to identify all the possible risks they face, then decide upon preventive measures to eliminate or reduce the impact of the risks.

Pure Risk:

It is uncertainty as to whether some unpredictable event that can result in loss will occur. Pure risk can result only in loss, never in gain. This kind of risk consists of hazards such as a fire or a hurricane, death of key employees, or customer injuries on the premises of the business. Pure risk exists when the possibility of loss is present, but the extent of the possible loss is unknown. Pure risk is different from speculative risk because speculative risk carries the possibility of gain as well as loss.

When we start a business, we automatically assume risk; we intend to make money, but we also know that we can lose money. Not starting a business at all is the only sure way to avoid the risk. Successful business man however, take control over how much risk they are willing to accept and then develop plans to control the remaining risks.

Businesses face many kinds of risks, and we should realize that there is no way to avoid all of them. Sound business management procedures can minimize the losses our business may suffer from some risks, but no amount of caution and planning can eliminate risk entirely.

As a business entity, we must be able to identify the risks that our business faces and take appropriate preventive measures to minimize losses. In addition, we should be aware of which losses we can protect your self from by

purchasing the appropriate business insurance. Otherwise, a lifetime of work and dreams can be lost in a few minutes.

Risk should not paralyze the zeal and enthusiasm of new business or project entities. They must be willing to take moderate risks when they believe there is a strong likelihood that they will succeed.

Speculative Risk:

It is uncertainty as to whether an activity will result in a gain or a loss. Risks, such as building a plant that turns out to have the wrong capacity or keeping an inventory level that turns out to be too high or too low, are speculative risks. Speculative risk is unavoidable and is inherent in the nature of the private enterprise system.

Cost of Risk

Risk management involves a holistic perspective of an organization in order to control events and arrange financing for expenses that may negatively impact its efficiency or impede achievement of corporate goals, such as continuity, stability, market share, dividend return, and growth. It is a financial function that must interface and have knowledge of business activities at the operating level.

The business sector was first to develop a comprehensive, system approach to risk due to the fiscal implications of "pure" loss on its financial statement. Risk was usually defined as an insurable or uninsurable hazard. Pure loss is defined as expenditures that have no opportunity for financial gain. Risk can be defined as uncertainty of loss.

Risk management is the continuing process to identify, analyze, evaluate, and treat loss exposures and monitor risk control and financial resources to mitigate the adverse effects of loss.

Loss may result from the following:

- Financial risks such as changing interest rates, exchange rates, receivables, equities

- Operational risks such as labor strikes
- Perimeter risks including weather or political change
- Strategic risks including management changes or loss of reputation

Avoiding or reducing the cost of loss is seen as a source of profit when it requires less expenditures than funding claims through the insurance marketplace or with internal funds and staff resources.

A current "buzz" word, Enterprise Risk Management, expands the province of risk management to define risk as anything that can prevent the company from achieving its objectives.

Although accidental losses are unforeseen and unplanned, there are methods which can make events more predictable. The more predictable an event, the less risk is involved since the occurrence can prevented or mitigated; or, at minimum, expenses can be estimated and budgeted. It is this process to make loss more predictable that is at the heart of the insurance industry.

The key to an economical and efficient risk program is control over the risk management functions with assurance that actions performed are desirable, necessary, and effective to reduce the overall cost of operational risk.

A risk management program is formulated and evaluated around the cost of risk.

The cost of Risk is comprised of:

- Retained Losses - Deductibles, Retention or Exclusions
- Net Insurance Proceeds
- Cost for Loss Control Activities
- Claim Management Expense
- Administrative Cost to Manage the Program

The benefits of a risk program should result in overall savings to the corporate entity when evaluating these components in the aggregate. Any one specific category may show an increase or decrease in cost when considered individually or by division in a specific time frame.

Risk Management Process

There are six major steps in risk management Process . The steps 2 to 6 are not one-off events and are repeated throughout the project. The steps 2 to 4 are collectively called assessment.

1. **Establish the context**

Define and identify the organization and project environments, characteristics, dependencies and stakeholders, their goals and objectives, and the scope and boundaries of the specific risk management process. Develop criteria against which risks are evaluated and identify the structure for risk management. Ensure all assumptions are recorded in the Project Charter or Assumptions List. When the context has been established then the Risk Management Plan can be prepared.

Purpose

The purpose of this step is to establish, for the project or program, the parameters for risk management and the criteria against which risks will be assessed.

The first step is to establish the strategic, organizational and risk management context in which the rest of the risk management process will occur. The starting point for this is the organization's enterprise level risk management policies and processes.

The strategic and organizational context is the relationship between the organization and its environment, characteristics and functions. Stakeholders must be identified. Risk management takes place in this wider context. Understanding this helps to identify and assess risks and plan acceptable treatments.

The specific project risk management context must also be established. This identifies the boundaries of the risk management activities and the necessary risk interfaces with other projects and organizations.

Risk management must be appropriate to the overall risk exposure. One approach for smaller projects is to undertake a 'flash' assessment to identify any

significant risks. The results of this will determine the subsequent scope of risk management activity. For some projects regular independent external reviews may be appropriate as a strategic risk treatment.

The project context leads to the appropriate level of risk management effort and initiates the Risk Management Plan.

Outputs

Initial version of the Risk Management Plan including the risk management policy for the project or program.

The key elements in establishing the risk context for a project:

- Establish the strategic context.
- Establish the organizational context.
- Establish the risk management context.
- Prepare the initial version of the Risk Management Plan.

2. **Identify and define risks.**

The project's risks are best identified through a collaborative approach involving a wide cross section of stakeholders in the project and recorded in the project's Risk Register. At the start of each project phase, the risks associated with that phase are formally identified through a similar process. All conceivable risks, including 'show stoppers', must be considered. Ensure any certainties are identified as problems and addressed in the project processes.

Purpose

The purpose of risk identification is to identify and define the positive and negative risks that may affect the project or program.

The identification of the risks associated with a project should start when the concept for the project is first developed. Risks are uncertainties affecting the achievement of the project's objectives. It therefore follows that risks cannot be fully identified if objectives are unclear. The project's Business Case must identify all known risks that may affect the complete life cycle from concept to eventual disposal of the system delivered by the project. The project's cost

benefit analysis must consider the estimated life cycle costs for the management of those risks from initiation onwards. At this stage the project's Risk Register (part of the Risk Management Plan) must be opened, and for larger projects an Assumptions List should also be created.

Unidentified risks cannot be managed. Effective risk identification must overcome barriers such as a 'can-do' or 'she'll be right' attitude, the unthinkable must be considered and not seen as 'undermining' or 'negative thinking'. A typical failing in risk identification is to focus on the easy and minor problems and ignore the potential 'show-stoppers'. One effective approach to catastrophic risks is to start with the catastrophe and work back to its sources.

Risk management is a continuous process, it is an inherent component of analysis, design, implementation and in-service support planning of any ICT system. Risks will change during these activities; risk estimates will be refined, some risks will disappear and new ones will emerge.

Risk management is an integral part of requirements engineering. This means applying it during analysis, synthesis, trade-offs and architectural design during the system engineering processes and to software architectural and detailed designs. Established techniques such as Event Trees, Fault Trees, Master Logic Diagrams, Event Sequence Diagrams, Reliability Block Diagrams, Failure Modes and Effects Analysis, and Failure Modes and Effects Criticality may be applicable.

In addition to embedding risk management into all aspects of a project, the Risk Register should be periodically reviewed as a formal activity established by the Risk Management Plan. This should be at milestones, particularly at the start of stages, but for larger and longer projects should be periodic, no less frequent than every two months.

Effective methods of risk identification include:

- Brainstorming, with a facilitator and range of stakeholders.
- Interviews with stakeholders.
- Scenario, business analysis and event tree modeling.
- Dependency modeling.

- Experience from other projects, metrics and published data for norms.
- Reviewing project information including plans, analysis and designs.

The key elements in the identification of a project's risks:

- Identify risks in the initial and revised business cases.
- Review risks throughout the project in accordance with the Risk Management Plan Document identified risks in the Risk Register.
- Encourage wide participation.
- Use a formal process and appropriate methods and techniques.
- Consider all risk sources

3. Conduct risk analysis

An analysis of the risks is conducted to determine their causes, and estimate their probability and consequences.

Purpose

The purpose of risk analysis is to consider all identified or changed risks to produce valid input for decision making in the evaluation step.

The analysis of the risks associated with a project requires high levels of participation by key representatives of the business, project team and other stakeholders. Risk analysis can be undertaken using similar methods as used for risk identification. Risk analysis is also a continuous process in the same way that risk identification is and the two may often be combined, in a structured way, into one activity.

Project or program risks are analyzed to identify the:

- Estimated likelihood that the risk will occur (preferably probability using quantitative methods);
- Estimated consequences of the risk occurring in terms of its cost, schedule, 'quality' and other impacts on the project objectives including its products;

- The most appropriate risk owner; and
- Potential impact of the risk on third parties such as other projects and organizations.

It can also be useful at this stage of the analysis to conduct an initial high level assessment of whether the risk should be managed.

There are four cases where a risk may not need managing by a project:

- The likelihood of it happening is extremely small.
- The consequences make the project irrelevant
- The consequences are insignificant and require no treatment
- The risk belongs outside the project; in this case the outside owners must formally take responsibility for it.

Wherever possible, the consequences of each risk should be valued. This is the risk exposure. At its simplest risk exposure = likelihood × consequence value. This is difficult to represent meaningfully using qualitative values such as 'high' and 'low', although these can be assigned numeric values to provide an interval scale. However, a more powerful quantification technique is to apply probabilities.

Where the consequences cannot be quantified they are normally qualitatively estimated on a scale from low to high or similar. A qualitative approach to both likelihood and consequences may be the only option at the very earliest stages of a project, but should migrate to quantitative as soon as possible. Qualitative estimates should use the 'most likely' (ie not best or worst case) criterion for rating the likelihood and consequences of a risk.

When considering the likelihood of a risk that is outside the project schedule then a time-period usually needs to be adopted. Typically the product's expected life but possibly some term such as 5 years, whole-life cost time frame or the period used for benefits realization. In some instances, particularly ICT security, it may be appropriate to consider vulnerability to a risk as part of its probability, including representing vulnerability as a risk source.

When analyzing risks it is important to document the information and assumptions underpinning the analysis, including the interdependencies between risks. This facilitates subsequent reviews and assessment changes.

Outputs

Estimates of the likelihood and consequences of risks and identification of the Risk Owners documented in the Risk Register.

The key elements in the analysis of a project's risks:

- Estimate the likelihood and consequences of each risk and the resultant risk exposure.
- Identify the most appropriate Risk Owner for each risk and assign the risk to them.
- Document the outcome of risk analysis in the Risk Register.

4. **Conduct risk evaluation**

The risks are considered and prioritized according to their potential impact on the business and the project, and each risk is assessed to determine its level of acceptability. The Risk Register is updated with the outcomes of the risk analysis and assessment process and identifies the risks that require management and assigns owners to them.

Purpose

The purpose of risk evaluation is to decide which risks need treatment and their priorities.

Once an analysis or review has been made of the risks associated with a project, the risks are evaluated to determine their treatment. The first action is to sort the analyzed risks by classifying them as one of:

- Accepted Risks, risks that are currently acceptable and do not require treatment, but will be kept under review.

- Rejected Risks, risks that are considered non-existent after analysis or of no significance.

Significant Risks to be treated, these may need prioritization. Classification and prioritization will be against risk criteria in the light of contexts and policies established in the Risk Management Plan. It is important to remember that one risk source may have several consequences, direct or chained, and that there will be inter-relationships between risks. These will affect the significance of risk sources and their impacts.

Evaluation should also consider the sensitivity of the estimates to errors. This is significantly less of an issue when estimates have the form of a probability distribution because quantitative methods facilitate it.

Optimism bias is another consideration, and reflects a human tendency to optimism. Quantitative methods can reduce this bias, which can be significant when project team members make the estimates. Other solutions include applying to estimates standard 'multipliers' derived from experience with similar projects or ensuring a process of rigorous independent review of risk identification and analysis.

In some instances it may be necessary to develop contingency plans:

- In case the risk eventuates;
- A critical decision point is reached without effective treatments being found; or
- There is a likelihood that an effective risk treatment will not be found.

When a risk has not been treated in a way that entirely eliminates it, then indicators of the risk eventuating may need to be identified. Manifestation of the indicators means that the likelihood of the risk is increasing and contingency plans may need to be executed.

If risks are positive then treatments should endeavor to make them more likely to occur or enhance their beneficial impact.

Treatments may have Secondary Risks, which must be analyzed and evaluated. Most typically where treatment involves re-work or additional work that affects cost, schedule, performance, scope or quality.

Accepted risks require a Risk Owner who is responsible for reviewing and monitoring them and reporting any changes that affect their likelihood or consequences.

In some instances a risk can be so severe that the viability of the project may need to be reassessed. These risks must be highlighted and formally considered by the Sponsor and, depending on the scale of the project and agency procedures, senior management up to chief executive officer (CEO) level to decide the appropriate action.

Outputs

The outcome of the risk evaluation is an updated Risk Register. This is reviewed by the Sponsor. Any changes to risk must be fully reflected in approved revisions of the business case.

The key elements in the evaluation of a project's risks:

- Classify the risks.
- Prioritize significant risks.
- Update the Risk Register.

5. **Develop and implement risk treatments**

Risk treatments are developed to cost-effectively reduce, contain and control project risk. Formal risk management reporting mechanisms are also defined.

Purpose

The purpose of this step is to identify, assess and implement measures to modify risks.

The Risk Owners prepare treatments for the risks assigned to them. Risk Owners may be members of the project team, business or other managers elsewhere in the agency, participating agencies or other stakeholder bodies. They will require an appropriate allocation of resources for their task(s), which may require negotiation by the Sponsor depending on their relationship to the project.

Treatments will either reduce the risk's likelihood or consequences or both. Preparation of treatments usually requires inputs from stakeholders and coordination with the Project Manager and Risk Manager. If there is an unacceptable risk of treatment failing (or not being found) or when a risk may reach an unacceptable level then a contingency plan must be developed. Secondary risks may be a consequence of risk treatment and may necessitate their own treatment or contingency plans.

Risk treatment has both tangible and intangible costs and care must be taken to ensure that the cost of treating a risk does not exceed its anticipated impact. This means that treatments must be costed, cost-effective and practical.

In some cases risk treatments will be embedded in the project. For example the risk of project estimating errors is best handled quantitatively and treated by appropriate allowance in the project schedule and cost plan. However, there is then a risk of self-fulfilling worst case prophecies, which have to be managed by setting 'stretch' targets and carefully selected 'must achieve' milestones. This is best done in a staged project design.

The major approaches for treating negative risks are:

- **Reduce likelihood**, where the project or its environment is changed to reduce the probability of a risk occurring;

- **Reduce consequences**, where action is taken to minimize the impact of a risk if it occurs. Treatment includes contingency planning that should address significant risk areas where preventive action is either unavailable or the cost of prevention is prohibitive;

- **Avoid risk**, by not proceeding with the aspect that may suffer the risk event;

- **Risk transfer**, where the responsibility for a risk is transferred to another party such as a supplier or insurance.

A range of treatments may be available for each risk and the Risk Owner must assess each option. Risk treatments may be reflected in project planning and can affect cost and schedule. However, early action may permit them to be

undertaken as modified future activities without cost or schedule impacts. Risks that are identified later in a project's implementation stage are more likely to have a significant impact on costs and schedule. It may be necessary to update the project's cost benefit analysis to reflect the anticipated costs of the risk treatments.

For each risk that is to be treated the risk treatments should identify:

- The Risk Owner responsible for treating the risk;
- Any relationships between risks;
- Indicators of the risk increasing or decreasing;
- The approach to be used to treat the risk;
- Assessment of the likelihood of the treatment being effective and mechanisms for measuring the effectiveness of the risk treatments;
- If necessary, a contingency plan, including an implementation decision point, if the risk treatment is insufficiently effective;
- The budget for the treatment; and
- If appropriate a time-scale for the completion of the risk treatment.

The risk treatments must be integrated with the overall project plan. This will ensure that any dependencies or potential resource conflicts between project tasks and risk treatments are identified and resolved. Where appropriate, the risk treatments should be linked to other business plans within the agency such as the corporate risk management plan.

Formal risk treatment reporting mechanisms should also be developed. Risk treatment must bv monitored by the Risk Manager and incorporated with the regular project progress reporting to the project's Sponsor and agency management as applicable.

Outputs

Planned treatment action for all risks that are not accepted and the Risk Register and project plans appropriately updated.

The key elements in the development and implementation of risk treatments:

- Identify risk treatments options.
- Assess each treatment including the need for contingency plans.
- Integrate treatments into the project plans.
- Document and cost risk treatments.
- Develop risk reporting mechanisms to the Sponsor and other stakeholders in accordance with agency delegations and procedures.

6. **Monitor, report, update and manage risks.**

As risks change during the project, the risk profile is continuously monitored, reviewed and updated. New risks may be identified as more information becomes available and existing risks may be eliminated through the effectiveness of the risk treatments.

Risk management is an essential component in the successful management of any project, whatever its size. It is a process that must start from the inception of the project, and continue until the project is completed and its expected benefits realized. Risk management is a process that is used throughout a project and its products' life cycles. It is useable by all activities in a project. Risk management must be focused on the areas of highest risk within the project, with continual monitoring of other areas of the project to identify any new or changing risks.

The success of a project's risk management strategies is dependent on:

- The commitment of the Sponsor and senior management to the risk management process;
- The skills and experience of the project team in the assessment of risks and the development of effective risk treatments;
- The project team, the business and other stakeholders working closely together to identify and manage all risks affecting the project;
- The use of an appropriate risk management process, methods and techniques continuously throughout the project;

- Regular reporting of performance against risk treatments, with this reporting provided by the project team and through appropriate independent quality assurance processes.

Purpose

The purpose of this step is to monitor and report on the effectiveness of all steps in the risk management process.

All projects should have a Risk Manager role. The person with this role has overall responsibility and authority for ensuring that the risk management process operates effectively in accordance with the project plans including the Risk Management Plan. This role should also seek continuous improvement to the project's risk management processes and enable other projects to learn from their experience. However, this role is not the owner of all risks.

It is at least highly desirable that when a contractor is undertaking any part of the work then their risk management is appropriately integrated with that of the customer agency. This may be achieved through a joint register of risks and its regular review, although both parties may have additional risks in their own registers. Of course a shared list of risks does not mean a shared responsibility for managing them. The extent of a contractor's risk reporting to the customer will depend on what is agreed in the contract.

As a project progresses its risks will change due to unforeseen factors. These include new or revised business requirements, changes in legislation or a supplier no longer able to provide a particular product. It is therefore essential that the project's risks are continuously monitored, regularly reviewed and updated. The frequency of these reviews depends on the duration of the project but should be a mixture of periodic and event based reviews. On larger projects they should be no less frequent that every two months.

Particular care must be taken to reassess risks to a project when:

- A new stage of the project starts;
- There is a significant change in the scope or approach of the project; or

- A substantial change occurs in the project's stakeholders or environment such as a new Sponsor or Project Manager.

Review of risks may lead to the:

- Identification of new risks;
- Elimination of risks that no longer apply; and
- Reclassification of existing risks where the estimated likelihood or impact has either increased or reduced.

Care must be taken to ensure that project management attention is not overly focused on areas that were initially assessed to be high risk. This may result in a failure to detect the emergence of new risks or the escalation of existing risks in other areas.

The assessment of any newly identified or changed risks is conducted in the same manner as described in the earlier sections of this Guideline. The outcome of this process is used to update the Risk Register. The risk treatments are also updated or new ones created to reflect the new or revised risks treatments that are to be adopted for the project. Ensure that changes to risk are fully reflected in any updates of the Business Case provided for Gateway Reviews.

Formal risk reporting arrangements to the appropriate organizational level must be established. Risk reports must highlight changed risks and contain relevant and concise information that can be efficiently assimilated by the reports' audience.

Risk monitoring and reporting needs to address two matters:

- Progress in the treatment of significant identified risks, including any indications that treatments may fail.

- Monitoring the project for indicators of other risks, that may or may not have been identified, emerging or growing. This involves analysis of project metrics, and when the risk has been identified its indicators should be recorded in the Risk Register.

Outputs

Updated Risk Register and reports as required by the Risk Management Plan.

The key elements in monitoring and updating a project's risk profile:

- There must be an overall Risk Manager.
- Regularly review the risks.
- Monitor the emergence of new or changing risks.
- Update the risk treatments.
- Maintain the Risk Register.

Risk Reports to appropriate recipients including the Sponsor and management in accordance with agency delegations and procedures. One thing should be made very clear at this point. Risk management is not a fancy word for safety. If Risk management is performed correctly and is conducted on a daily basis the end result of your efforts is safety.

Contributions of Risk Management to Business, Society and Family

Business Risk Management

Understanding business risk requires three criteria:

1. A thorough understanding of the business process
2. An active imagination and tools to generate ideas about possible effects of risks.
3. A framework or risk model and a common language to discuss risk

A thorough understanding of the business process implies a collaborative approach to understanding risk management. These first two criteria, business knowledge and the means to tap the imagination, could create chaos without some means of organizing and communicating that knowledge.

We can follow a risk model which is a logical algorithm or formula that can model the total business risk in each of the organization's business processes and projects. Most people have an intuitive understanding of risk based on their

common sense and experience. Perhaps it is this common-sense approach that lulls us into false comfort. Obvious risks are no real threat, given a reasonably alert management. However, it is unintended consequences that challenge our common sense and experience. An integrated framework of risk ensures that the blended knowledge and experience from our collaborative efforts can be organized and communicated to top management in a language that all understand. Such a framework needs to be both complete and flexible so that it adapts to all types of organizations.

The framework needs to address all of the assets at risk in the organization. These are:

- **Financial:** Cash, credit and negotiable instruments.
- **Physical:** Land, buildings and equipment.
- **Human:** Knowledge, skills and commitment of people.
- **Intangible:** Reputation, brand and information.

Finally, the framework needs to include the element of time. The consequences of some risk events vary with their duration. Some processes are sensitive to delay. Subtle risks, such as obsolescence and opportunity costs, also should be included in the framework.

The framework of business risk management is composed of three major domains of business risk and a number of risk groups within each domain. Some risk groups are shared between domains. The three domains of business risk are defined as:

- **Ownership Risks:** The risks associated with acquiring, maintaining and disposing of assets (all except human assets).

- **Process Risks:** The risks associated with putting assets to work to achieve objectives.

- **Behavioral Risks:** The risks associated with both acquiring, maintaining and disposing of human assets.

Each risk group is a collection of specific business risks, some of which are common to all organizations, and some are industry-specific. Examples of

common specific risks in a group are the risks associated with Dysfunctional Workplaces. Industry-common risks include harassment, theft, sabotage, injury, employee lawsuits, violence, and other similar risks. Industry-specific risks associated with External Threats would be different for banking, public sector agencies, manufacturing, etc. depending upon the nature of their markets, the extent of government regulation, their customer/constituent segment, the nature of their technology and its rate of change, and similar external threats.

Elements of the Framework

Ownership risks include the following:

- External Threats: Forces outside of the control of the organization that can affect the organization's business processes and goals. Examples include customer/constituent demands, labor/financial/product markets, suppliers (including unions), competitors, government regulation, economic/political forces, technology, physical / environmental forces.

- Custodial Risks: The risks associated with owning and safeguarding assets. Since human assets have different characteristics, that class is covered under Behavioral Risks. Examples of custodial risks include obsolescence, damage in handling or storing the assets, and theft from storage.

- Hazards (shared with Process Risks): The risks to assets associated with loss or impairment through fire and natural or man-made disasters and accidental loss.

- Opportunity Costs (shared with Behavioral Risks): The cost of making less-than-optimum decisions about asset acquisition and disposition. Examples include purchasing the wrong asset, paying too much, selling the asset too soon or too late, selling the asset too cheaply, and disposing of the wrong asset.

Process risks include the following:

- Hazards (shared with Custodial Risks): The risks to processes associated with loss or impairment through fire and natural or man-made disasters and accidental loss.

- Errors/Omissions/Delays: The risks to processes arising from random differences in human or machine activity in the process. Poor judgment in plans or operations, inappropriate or outdated control mechanisms, and machine malfunction are examples of these risks.

- Frauds: The risk to processes arising from intentional misrepresentation of suppliers, employees and customers. Examples of these risks include theft, bid rigging, bribery, kick-back schemes, and customer abuse.

- Productivity Loss (shared with Behavioral Risks): The risks to the process arising from poor design of the process or its control system. Examples include scheduling conflicts, inappropriate work rules, missing controls, lack of monitoring control systems, under-utilizing assets in the process, and goal conflicts.

Behavioral risks include the following:

- Productivity Loss (shared with Process Risks): The risks arising from poor management practices or poor worker commitment. Under-utilizing human assets, poor leadership, favoritism, lack of work structure and discipline, inconsistent management decisions, and personal/work goal conflicts are examples of these risks.

- Dysfunctional Workplaces: The risks to employees from a dysfunctional work environment, and the risks to the organization from employees working in such an environment. Examples of these risks are gender/racial harassment, excessive pressure to meet objectives (without compensating relief valves), employee theft and sabotage, workplace injuries, employee lawsuits, and workplace violence.

- Opportunity Costs (shared with Ownership Risks): The cost of making less-than-optimum decisions about human asset (people, knowledge, and skills) acquisition and disposition. Hiring the wrong people or skills, a poor compensation system, and letting the wrong people or skills leave the organization (through quitting, firing or outsourcing) are examples of such risks.

Managing Risk

Common risk management techniques include:

- **Avoid:** Redesign the process to avoid particular risks with the plan of reducing overall risk.
- **Diversify:** Spread the risk among numerous assets or processes to reduce the overall risk of loss or impairment.
- **Control:** Design activities to prevent, detect or contain adverse events or to promote positive outcomes.
- **Share:** Distribute a portion of the risk through a contract with another party, such as insurance.
- **Transfer:** Distribute all of the risk through a contract with another party, such as outsourcing.
- **Accept:** Allow minor risks to exist to avoid spending more on managing the risks than the potential harm.

All risk management techniques are found in all domains; however, there are some primary risk management strategies. Many ownership risks are insurable risks, and the primary risk management strategy is risk transfer or risk sharing through insurance. Process risks are primarily managed through an active system of internal controls in the processes, including active management oversight. Behavioral risks are perhaps the most varied and most difficult. Primary risk management techniques for behavioral risks are avoidance (redesign the workplace to reduce the level of risk) and risk transfer (workers compensation and liability insurance). Management is about managing business risks. An integrated risk management approach using a number of techniques is necessary to cover the full range of risks in the framework.

A framework of business risk can provide a common ground for managers, auditors and other stakeholders to establish effective and efficient risk management for their organization. The framework is useful also as a template or tool to stimulate the imagination about how the organization achieves its goals

in an uncertain environment. With a common language, imagination and a thorough knowledge of the business process, the organization is more likely to achieve its business goals.

Review Questions:

1. What is risk management?
2. Define the concept of risk.
3. What are the objectives of risk management?
4. Explain the classification of risk.
5. What is pure risk?
6. What is speculative risk?
7. Define cost of risk.
8. Explain the risk management process.
9. Describe the contributions of risk management to business.
10. Describe the contributions of risk management to society.

* * *

UNIT 2

RISK MANAGEMENT IN BUSINESS

Business requirements are changing, forcing organizations to take a hard look at their round the-clock operations and growing service-level expectations. Add to this equation the emergence of closer regulatory scrutiny and stringent out-of-region data protection requirements, and it becomes clear that the increased sensitivity to loss of information assets is not going to subside any time soon. Is this necessarily a bad thing? After all, the challenge is to understand and reduce risk…and increase business resilience.

Credit Risk (including Settlement Risk)

Broadly defined, credit risk is the risk that counterparty will fail to perform on an obligation to the institution. The institution should evaluate both settlement and pre-settlement credit risk at the customer level across all products. On settlement day, the exposure to counterparty default may equal the full value of any cash flows or securities the institution is to receive. Prior to settlement, credit risk is measured as the sum of the replacement cost of the position, plus an estimate of the institution's potential future exposure from the instrument as a result of market changes. Replacement cost should be determined using current market prices or generally accepted approaches for estimating the present value of future payments required under each contract, given current market conditions.

Potential credit risk exposure is measured more subjectively than current exposure and is primarily a function of the time remaining to maturity and the expected volatility of the price, rate or index underlying the contract. Dealers and large derivatives participants should assess potential exposure through simulation analysis or other sophisticated techniques, which, when properly designed and implemented can produce estimates of potential exposure that incorporate both portfolio-specific characteristics and current market conditions. Smaller end-users may measure this exposure by using ";add-ons" based on more general characteristics. In either case, the assumptions underlying the institution's risk measure should be reasonable and if the institution measures exposures using a portfolio approach, it should do so in a prudent manner.

An institution may use master netting agreements and various credit enhancements, such as collateral or third-party guarantees, to reduce its counterparty credit risk. In such cases, an institution's credit exposures should reflect these risk-reducing features only to the extent that the agreements and recourse provisions are legally enforceable in all relevant jurisdictions. This legal enforceability should extend to any insolvency proceedings of the counterparty. The institution should be able to demonstrate that it has exercised due diligence in evaluating the enforceability of these contracts and that individual transactions have been executed in a manner that provides adequate protection to the institution.

Credit limits that consider both settlement and pre-settlement exposures should be established for all counterparties with whom the institution conducts business. As a matter of general policy, business with counterparty should not commence until a credit line has been approved. The structure of the credit-approval process may differ among institutions, reflecting the organizational and geographic structure of each institution. Nevertheless, in all cases, it is important that credit limits be determined by personnel who are independent of the derivatives function, that these personnel use standards consistent with those used for other activities and that counterparty credit lines are consistent with the organization's policies and consolidated exposures.

If credit limits are exceeded, exceptions should be resolved according to the institution's policies and procedures. In addition, the institution's reports should adequately provide traders and credit officers with relevant, accurate and timely information about the credit exposures and approved credit lines.

Similar to bank loans, OTC derivatives products can have credit exposures existing for an extended period. Given these potentially long-term exposures and the complexity associated with some derivatives instruments, an institution should consider the overall financial strength of its counterparties and their ability to perform on their obligations.

Market Risk

Market risk is the risk to an institution's financial condition resulting from adverse movements in the level or volatility of market prices. The market

risks created - or hedged - by a future or swap are familiar, although not necessarily straightforward to manage. They are exposures to changes in the price of the underlying cash instrument and to changes in interest rates. By contrast, the value of an option is also affected by other factors, including the volatility of the price of the underlying instrument and the passage of time. In addition, all trading activities are affected by market liquidity and by local or world political and economic events.

Market risk is increasingly measured by market participants using a value-at-risk approach, which measures the potential gain or loss in a position, portfolio or institution that is associated with a price movement of a given probability over a specified time horizon. The institution should revalue all trading portfolios and calculate its exposures at least daily. Although an institution may use risk measures other than value-at-risk, the measure used should be sufficiently accurate and rigorous, and the institution should ensure that it is adequately incorporated into its risk management process.

An institution should compare its estimated market risk exposures with actual behaviour. In particular, the output of any market risk models that require simulations or forecasts of future prices should be compared with actual results. If the projected and actual results differ materially, the assumptions used to derive the projections should be carefully reviewed or the models should be modified, as appropriate.

The institution should establish limits for market risk that relate to its risk measures and that are consistent with maximum exposures authorized by its senior management and board of directors. These limits should be allocated to business units and individual decision makers and be clearly understood by all relevant parties. Exceptions to limits should be detected and adequately addressed by management. In practice, some limit systems may include additional elements such as stop-loss limits and guidelines that may play an important role in controlling risks.

An institution whose derivatives activities are limited in volume and confined to end-user activities may need less sophisticated risk measurement systems than those required by a dealer. Senior management at such an institution should ensure that all significant risks arising from its derivatives

transactions can be quantified, monitored and controlled. At a minimum, risk management systems should evaluate the possible impact on the institution's earnings and capital which may result from adverse changes in interest rates and other market conditions that are relevant to risk exposure and the effectiveness of derivatives transactions in the institution's overall risk management.

Liquidity Risk

An institution faces two types of liquidity risk in its derivatives activities: one related to specific products or markets and the other related to the general funding of the institution's derivatives activities. The former is the risk that an institution may not be able to, or cannot easily, unwind or offset a particular position at or near the previous market price because of inadequate market depth or because of disruptions in the marketplace. Funding liquidity risk is the risk that the institution will be unable to meet its payment obligations on settlement dates or in the event of margin calls. Because neither type of liquidity risk is necessarily unique to derivatives activities, management should evaluate these risks in the broader context of the institution's overall liquidity. When establishing limits, the institution should be aware of the size, depth and liquidity of the particular market and establish guidelines accordingly.

In developing guidelines for controlling liquidity risks, an institution should consider the possibility that it could lose access to one or more markets, either because of concerns about the institution's own creditworthiness, the creditworthiness of a major counterparty or because of generally stressful market conditions. At such times, the institution may have less flexibility in managing its market, credit and liquidity risk exposures. An institution that makes markets in over-the-counter derivatives or that dynamically hedges its positions requires constant access to financial markets and that need may increase in times of market stress. The institution's liquidity plan should reflect the institution's ability to turn to alternative markets, such as futures or cash markets, or to provide sufficient collateral or other credit enhancements in order to continue trading under a broad range of scenarios.

An institution that participates in over-the-counter derivatives markets should assess the potential liquidity risks associated with the early termination of derivatives contracts. Many forms of standardized contracts for derivatives

transactions allow counterparties to request collateral or to terminate their contracts early if the institution experiences an adverse credit event or a deterioration in its financial condition. In addition, under conditions of market stress, customers may ask for the early termination of some contracts within the context of the dealer's market making activities. In such situations, an institution that owes money on derivatives transactions may be required to deliver collateral or settle a contract early and possibly at a time when the institution may face other funding and liquidity pressures. Early terminations may also open up additional, unintended, market positions. Management and directors should be aware of these potential liquidity risks and should address them in the institution's liquidity plan and in the broader context of the institution's liquidity management process.

Operations Risk

Operations risk is the risk that deficiencies in information systems or internal controls will result in unexpected loss. This risk is associated with human error, system failures and inadequate procedures and controls. This risk can be exacerbated in the case of certain derivatives because of the complex nature of their payment structures and calculation of their values.

The board of directors and senior management should ensure the proper dedication of resources (financial and personnel) to support operations and systems development and maintenance. The operations unit for derivatives activities, consistent with other trading and investment activities should report to an independent unit and should be managed independently of the business unit. The sophistication of the systems support and operational capacity should be commensurate with the size and complexity of the derivatives business activity.

Systems support and operational capacity should be adequate to accommodate the types of derivatives activities in which the institution engages. This includes the ability to efficiently process and settle the volumes transacted through the business unit, to provide support for the complexity of the transactions booked and to provide accurate and timely input. Support systems and the systems developed to interface with the official databases should generate accurate information sufficient to allow business unit management and senior management to monitor risk exposures in a timely manner.

Systems needs for derivatives activities should be evaluated during the strategic planning process. Current and projected volumes should be considered together with the nature of the derivatives activity and the user's expectations. Consistent with other systems plans, a written contingency plan for derivatives products should be in place.

With the complexity of derivatives products and the size and rapidity of transactions, it is essential that operational units be able to capture all relevant details of transactions, identify errors and process payments or move assets quickly and accurately. This requires a staff of sufficient size, knowledge and experience to support the volume and type of transactions generated by the business unit. Management should develop appropriate hiring practices and compensation plans to recruit and retain high caliber staff.

Systems design and needs may vary according to the size and complexity of the derivatives business. However, each system should provide for accurate and timely processing and allow for proper risk exposure monitoring. Operational systems should be tailored to each institution's needs. Limited end-users of derivatives may not require the same degree of automation needed by more active trading institutions. All operational systems and units should adequately provide for basic processing, settlement and control of derivatives transactions.

The more sophisticated the institution's activity, the more need there is to establish automated systems to accommodate the complexity and volume of the deals transacted, to report position data accurately and to facilitate efficient reconciliation.

Segregation of operational duties, exposure reporting and risk monitoring from the business unit is critical to proper internal control. Proper internal control should be provided over the entry of transactions into the database, transaction numbering, date and time notation and the confirmation and settlement processes. Operational controls should also be in place to resolve disputes over contract specifications. In this regard, an institution must ensure that trades are confirmed as quickly as possible. The institution should monitor the consistency between the terms of a transaction as they were agreed upon and the terms as they were subsequently confirmed.

The operations department, or another unit or entity independent of the business unit, should be responsible for ensuring proper reconciliation of front and back office databases on a regular basis. This includes the verification of position data, profit and loss figures and transaction-by-transaction details.

The institution should ensure that the methods it uses to value its derivatives positions are appropriate and that the assumptions underlying those methods are reasonable. The pricing procedures and models the institution chooses should be consistently applied and well-documented. Models and supporting statistical analyses should be validated prior to use and as market conditions warrant.

Management of the institution should ensure that a mechanism exists whereby derivatives contract documentation is confirmed, maintained and safeguarded. An institution should establish a process through which documentation exceptions are monitored and resolved and appropriately reviewed by senior management and legal counsel. The institution should also have approved policies that specify documentation requirements for derivatives activities and formal procedures for saving and safeguarding important documents that are consistent with legal requirements and internal policies.

Although operations risks are difficult to quantify, they can often be evaluated by examining a series of "worst-case" or "what if" scenarios, such as a power loss, a doubling of transaction volume or a mistake found in the pricing software for collateral management. They can also be assessed through periodic reviews of procedures, documentation requirements, data processing systems, contingency plans and other operational practices. Such reviews may help to reduce the likelihood of errors and breakdowns in controls, improve the control of risk and the effectiveness of the limit system and prevent unsound marketing practices and the premature adoption of new products or lines of business. Considering the heavy reliance of derivatives activities on computerized systems, an institution must have plans that take into account potential problems with its normal processing procedures.

Legal Risk

Legal risk is the risk that contracts are not legally enforceable or documented correctly. Legal risks should be limited and managed through

policies developed by the institution's legal counsel (typically in consultation with officers in the risk management process) that have been approved by the institution's senior management and board of directors. At a minimum, there should be guidelines and processes in place to ensure the enforceability of counterparty agreements.

Prior to engaging in derivatives transactions, an institution should reasonably satisfy itself that its counterparties have the legal and necessary regulatory authority to engage in those transactions. In addition to determining the authority of a counterparty to enter into a derivatives transaction, an institution should also reasonably satisfy itself that the terms of any contract governing its derivatives activities with counterparty are legally sound.

An institution should adequately evaluate the enforceability of its agreements before individual transactions are consummated. Participants in the derivatives markets have experienced significant losses because they were unable to recover losses from a defaulting counterparty when a court held the counterparty had acted outside of its authority in entering into such transactions. An institution should ensure that its counterparties have the power and authority to enter into derivatives transactions and that the counterparties' obligations arising from them are enforceable. Similarly, an institution should also ensure that its rights with respect to any margin or collateral received from a counterparty are enforceable and exercisable.

The advantages of netting arrangements can include a reduction in credit and liquidity risks, the potential to do more business with existing counterparties within existing credit lines and a reduced need for collateral to support counterparty obligations. The institution should ascertain that its netting agreements are adequately documented and that they have been executed properly. Only when a netting arrangement is legally enforceable in all relevant jurisdictions should an institution monitor its credit and liquidity risks on a net basis.

The institution should have knowledge of relevant tax laws and interpretations governing the use of derivatives instruments. Knowledge of these laws is necessary not only for the institution's marketing activities but also for its own use of these products.

Scope of Risk Manager's Duties

The Risk Management Group will be responsible for progressing risk management within the Board and co-ordinating its roll-out. Initially it will identify strategic risks which will be of benefit to Heads of Division/Section.

The Accounting Officer is responsible for setting the tone and influencing the culture of risk management within the Board and will be kept up to date with developments through reports to the Senior Management Team.

Heads of Department will be responsible for ensuring that risk management is given appropriate resources to ensure full compliance within timescales set down.

Heads of Division and Section will be responsible for ensuring that the risk management process is undertaken within their areas of responsibility. They will be primarily responsible for identifying operational risks and taking into account strategic risks identified by the RMG. Each Division will maintain a risk register which will be used to build a Corporate Risk Register. Key risks and their controls will be monitored on an ongoing basis to determine whether Business Plan objectives are achievable.

Internal Audit will facilitate the risk management process through involvement in the RMG and workshops. Internal audit will carry out independent reviews of the effectiveness of risk management and control and report on these.

Reports on progress of the process will be made to appropriate committees and to the Audit Committee. The Audit Committee will scrutinize the progress reports to ensure the effectiveness of the risk management, control and governance systems.

It is the responsibility of the **project manager** to:

1. Understand the project requirements and ensure they are thoroughly and unambiguously documented;
2. Prepare a project plan with achievable cost, schedule, and performance goals;

3. Identify and manage project risks;
4. Ensure the project team is well-organized, adequately staffed, and working well together;
5. Manage project cost, schedule, requirements, and design baselines so they are traceable;
6. Report meaningful metrics for cost, schedule, quality, and risk;
7. Conduct regular status and design reviews;
8. Ensure the adequacy of project documentation and testing;
9. Maintain meaningful communications among project stakeholders; and
10. Manage the project to attain the project goals and achieve stakeholder satisfaction.

The person in the organization responsible for the project, above the project manager, is the **project sponsor**. It is the responsibility of the project sponsor to:

1. Select, develop, and guide, or change, the project manager to achieve project goals;
2. Hold the PM accountable for fulfilling the responsibilities listed above;
3. Support the PM in obtaining resources and tools needed to conduct the project;
4. Require regular status briefings and design reviews, and pass pertinent information up the line;
5. Advise the PM on conditions likely to cause project risks; and
6. Be an advocate for the PM and the project team.

The scope of risk manager includes:

- Determination value of business assets.
- Determine probability of impact on business assets.
- Designing technical solutions and estimate engineering costs.
- Designing of operational components of solution and estimating operating costs.

The following requirements need to be in place if risk management is to be effective and innovation encouraged;

(a) Risk management policies and benefits should be clearly communicated to all staff;

(b) Senior Management need to support and promote risk management;

(c) Board culture should support well thought through risk-taking and innovation;

(d) Risk management should be embedded in the management process;

(e) The management of risk should be clearly linked to the achievement of objectives; and

(f) Risks associated with working with other organizations should be assessed and managed.

RISK MANAGEMENT CORPORATE POLICY AND STRATEGY

a. Soundness and clarity of management policy

Check points		Specific sample questions
a. Soundness, rationality, and integrity of management policy	Has the management established a sound and rational policy (short- and long-term strategies) with full consideration given to current and future management conditions?	• When drawing up management policy, does the management take into consideration soundness, rationality, and feasibility? • Is the management policy integrated?
b. Clarity and permeability of management policy	Is the management policy clear and well understood, and does it function well?	• Is the management policy clear with respect to criteria for action by each department? • Is the policy well understood throughout the entire organization, and does it function well?

		• Does the bank compile a medium- and long-term business plan (e.g., every 3-5 years)? • Does the bank compile a business plan (annually or semiannually)? • Does the department in charge of management planning regularly monitor the level of accomplishment and make necessary adjustments?

b. Permeability of risk management policy

Check points		Specific sample questions
a. Understanding of risk management	Does the management accurately recognize the types of risk and risk exposure inherent in the bank's portfolio and understand the method of risk management, and has it encouraged the bank to establish full awareness of the importance of risk control throughout the bank?	• Does the management have high professional moral standards and make efforts to establish awareness of the importance of internal controls among employees? • Does the management recognize internal and external factors constituting potential risks to the bank, and is the management aware of the different types and degrees of risk and risk exposure inherent in these factors? • Does the management recognize different risk management methods according to the types of risk and risk exposure? • Does the management set limits to the acceptable amount or degree of risks inherent in the bank and adequately instruct relevant sections?

b. Basic strategy for risk management	Is the management actively involved in drawing up strategies and establishing the framework for risk management giving due consideration to the balance between various risks to the bank's capital and also the strategic importance of its risk-taking?	• Is the management clearly aware of its responsibility for drawing up appropriate and adequate risk management policy? • Does the board of directors decide basic policy vis-à-vis risk-taking and risk control giving due consideration to the balance between various risks to the bank's capital as well as each business operation? • Does the management regularly check the effectiveness of its risk management system? • Does the management possess the necessary framework, system, and procedures for identifying, monitoring, and controlling various risks? • Does the management aim to build a comprehensive risk management system on an institution-wide basis?
c. Diversification of risks	Does the bank diversify risks in the operation of its various businesses?	• Is the bank aware of the necessity of diversifying fund-raising sources and investment vehicles? • Does the bank have in place an organization and operational framework that further emphasizes the importance of risk management rules and regulations such as limit on exposure to a single borrower? • Does the bank avoid excessive dependency on a specific counterparty in its business operation? • Is it possible to monitor risks so as to detect any maldistribution?

d. Countermeasures against payment failure of other banks	Does the management understand the effects of payment failure by other banks and resulting instability of the financial system, and have in place appropriate countermeasures?	• Does the management clearly understand the loss-burden rule applying to payment and settlement systems such as the Zengin Data Telecommunications System (Zengin System), Foreign Exchange Yen Settlement System, and CD on-line tie-up, and implement appropriate countermeasures against inherent risks? • Does the bank have in place countermeasures against payment failure by other banks or resulting financial system instability?

B. Internal Controls

1. Organization, delegation of authority, and reporting system

Check points		Specific sample questions
a. Organization	Is the bank adapting its organization so as to strengthen the risk management system and to implement flexible countermeasures to meet changes in the financial environment?	• Is the bank adapting its organization and staff allocation so as to strengthen the risk management system? • Is the burden of responsibility regarding business operations and risk management clearly defined? • Does the bank have in place a system that can control risk exposure while responding to economic change by utilizing research department data? • Does the bank have in place an internal control system capable of swiftly and adequately dealing with newly recognized risks arising from changes in the environment, etc.?

		• Is the bank aware of the necessity for organizational reform in line with changes in the environment, etc., and is there a department responsible for planning and implementing measures in response to such changes? • Does the institution-wide risk management section regularly assess the effectiveness of the bank's overall risk control system?
b. Separation of responsi-bilities	Are the framework and procedures for decision-making clarified? Are delegation of authority and allocation of responsibilities conducted appropriately from the standpoint of securing a double-checking system and avoiding conflict of interest? Are these procedures clearly stipulated in the internal rules for delegation of authority?	• Are internal rules for the delegation of authority rational from the standpoint of securing double-checking of operations and risk control in line with business expansion? • Has the bank confirmed that there is no excessive concentration of authority nor extreme delegation of authority to subordinates? • Does the bank have in place a framework where monitoring and evaluation of major risks are conducted by a specializing section independent from the business promotion department? • Are risk management responsibilities clearly defined among the board of directors, ALM committee, directors in charge, and department heads? • Does the department head keep to the unavoidable minimum the range of duties where a sufficient double-checking system cannot be applied, and does the bank have in place a system for close monitoring?

c. Reporting of business information	Does the bank have in place an appropriate reporting system by which the management can receive valuable information on business operations and risk management? Are decisions made by the management clearly understood by the entire organization?	• Does the bank have in place an appropriate reporting system by which directors in charge and the board of directors receive information on business operations and risk management without undue delay? • Does the bank have a consistent reporting format, giving due consideration to easy comprehension and coherency of contents? • Are decisions made by directors in charge and the board of directors adequately communicated to, and understood by, concerned sections (including domestic and overseas branches)? • Does the bank have in place a regular reporting system to senior officers and management regarding risk management?

2. Staff recruitment and training

Check points		Specific sample questions
a. Staff recruitment	Does the bank recruit staff with appropriate experience, skill levels, and degree of expertise to undertake specialized business operations?	• Does the bank recruit staff with appropriate experience, skill levels, and degree of expertise to undertake specialized business operations, in particular, those relating to risk management? • Do staff members actively take part in business operations in line with their position and responsibilities? • Does the bank recruit staff based on an employment plan?

b. Training	Does the management have a clear policy on staff training?	• Does the on-the-job training (OJT) program function adequately? • Does the bank have training programs according to qualifications and job description? • Does the bank revise training programs in accordance with changes in business operation and sophistication of risk management?

3. Internal audit

Check points		Specific sample questions
a. Audit system	Does the bank conduct effective internal audits (headquarters audit and in-house audit) to enhance its risk management system and check the thoroughness of internal rules?	• Are the frequency, check points, and scope of internal audits adequate? • Does the internal audit section/department have auditors with expertise in each business area, and are they able to effectively audit the bank's overall operation? • Does the internal audit section/department have access to all relevant documents and vouchers? • Does the bank conduct regular internal audits of all departments including headquarters and of all operations excluding those which are considered customarily exempted from auditing? • Is the internal audit section/department completely independent from other sections/departments, and does it directly report to the management?

b. Follow-up of audit	Does the management give prompt and adequate attention to audit results, and take appropriate measures if problems are detected?	• Are internal audit results reported to the management promptly and accurately? • Is information useful for improvement of operations regularly passed on to concerned departments such as the operations planning department? • Does the internal audit section/department take the initiative in directing improvement measures such as the revision of internal rules in order to prevent the reoccurrence of problems? • Does the management appropriately monitor whether improvement measures directed to sections/departments are carried out?

C. Profit/Loss Management and Risk Management of Affiliated Companies

1. Profit/loss management

Check points		Specific sample questions
a. Monitoring of profit/loss	Do the management and individual departments within the organization monitor profit/loss while considering the balance between risk and return?	• Does a specialized department (e.g., the financial department) monitor profit/loss from various viewpoints such as profit by customer and branch, and on a consolidated basis? • Does each department manage profit/loss bearing in mind the allocation of indirect costs? • Is due consideration given to risk profiles when assessing and determining profit/loss conditions? • Is there a computerized support system for profit/loss management (e.g., cost accounting of deposits and lending)?

b. Distribution of management resources taking into account risk and return	Is due consideration given to the balance between risk and return, and between risk and the bank's capital when distributing management resources to each department?	• Does the bank thoroughly assess capital and other resources before embarking on a new business? • Does the management appropriately decide the resources distribution policy based on regular profit/loss reports? • Are limits on risk exposure set for each department taking into consideration the bank's capital?
c. Rational pricing	Is pricing of deposit and lending rates rational in view of operational/profit planning, market conditions, and risks?	• Is the differential between actual market rates and pricing of deposit, lending, and derivatives rates within a rational range? • Is delegation of authority relating to pricing clearly defined? • In pricing, is consideration given not only to operations, profit, and market conditions, but also operating cost, credit spread, and embedded option premium for premature cancellation?

2. Risk management of affiliated companies

Check points		Specific sample questions
a. Monitoring of profit/loss on a consolidated basis including affiliated companies	Is financial performance monitored appropriately on a consolidated basis or on the basis of including affiliated companies not subject to consolidated accounting?	• Is financial performance monitored on a consolidated basis with full understanding of the business performance of companies subject to consolidated accounting? • Is financial performance monitored appropriately on the basis of including affiliated companies not subject to consolidated accounting taking into consideration degree of business affiliation?

b. Risk management of affiliated companies	Does the head office fully recognize the risks inherent in domestic and overseas affiliated companies, and monitor them appropriately?	• Is there a section responsible for monitoring the business operations of affiliated companies (including non-bank financial institutions)? • Is the bank capable of checking unusual activities such as large fund transfers among affiliated companies? • Does the head office fully recognize the risk profiles inherent in overseas affiliated companies? • Does the bank regularly monitor risks to which domestic and overseas affiliated companies are exposed in order to ensure that they are within a rational range in proportion to their financial strength such as capital?

D. Compliance and Disclosure

1. Establishment of a framework for compliance

Check points		Specific sample questions
a. Management understanding of legal compliance and action to achieve it	Does the management fully recognize the importance of complying with laws and regulations, market rules, and internal rules? Are they taking the initiative in raising compliance awareness?	• Does the management fully understand that insufficient compliance can impair the management base? • Is the top management making efforts to ensure that recognition of the importance of compliance penetrates throughout the bank? • Is the management fully aware which bank operations are most likely to cause problems in terms of compliance? • When starting a new type of operation, does the management take into consideration of newly arising risks in the area of compliance?

b. Establish-ment and implementation of a framework for compliance	Has the bank established a framework and concrete procedures (a compliance program) to ensure consistent compliance? Are they appropriately implemented?	• Are responsibilities with respect to compliance made clear by appointing an executive director and setting up a coordination department in charge? Are matters related to the bank's compliance such as planning, proposals, and monitoring under centralized control? • Does the bank have in place concrete procedures (i.e., planning of education and training programs, compiling codes of conduct and compliance manuals, drawing up internal rules, etc.) which effectively initiate compliance? • Do banks with overseas branches have a compliance officer for each country who regularly collects information about changes in local legislation? • Has the bank appropriately placed a person in charge of compliance in relevant departments and clearly stipulated their job descriptions in the allocation of duties? Have these positions been effectively put into practice (i.e., implementation of training programs and educational activities, consultation, and inspection in the event of any doubtful contradictions to rules, swift reporting to the coordinating department)? • In the development and sales of new products, does the coordinating department confirm the legal compliance of its content and policy of customer explanation in advance? • Does the bank maintain close contact with its lawyers with a view to forestalling trouble and dealing with any incident appropriately and swiftly?

c. Monitoring and reporting to management	In addition to monitoring, does a department independent of operations sections conduct checks on compliance? Are lawsuits and problems that could harm the bank's reputation appropriately reported to the management?	• Is the compliance consistency in each type of bank business monitored by compliance officers and in-house audits on a daily basis? • Does the compliance officer promptly and appropriately report the compliance consistency and problems in each operation section to the coordinating department? • Does a department (i.e., internal audit department) independent from operation sections and a coordinating department regularly examine the compliance consistency? • Does the coordinating or internal audit department promptly and appropriately report the compliance consistency and problems to the management and auditors (or auditors committee)? • Are incidents and accidents swiftly reported to the supervisory authorities? Is the credibility of the content of reports sent to other authorities assured? • Are summaries of customer complaints or lawsuits sent to branches in order to forestall problems?

2. Disclosure and accounting process

Check points		Specific sample questions
a. Active disclosure of financial information and	From the standpoint of fulfilling accountability to customers and shareholders, does the	• Are the bank's management policy and strategies made widely known through disclosure magazines and other means? • Are major indicators of the bank's performance accurately disclosed?

restraints on manage-ment	management actively and fairly disclose financial information? Is the management sufficiently monitored internally and externally in order to secure business operations?	• Do the board of directors and auditors (or auditors committee) function appropriately to secure proper execution of business by the management? When required, does the bank appoint external board members and set up a compliance committee? • Does the management take due notice of the opinions of external auditors (letters of advice on improvement of internal control, i.e., management letters)? Does the management examine and implement appropriate improvement measures? • Does the bank actively initiate relations with investors, by for example, conducting briefings about its business performance for investors?
b. Appro-priate accounting procedures	Is the bank's processing of daily accounts and annual financial statements sound?	• Is the processing of daily accounts carried out properly? • Are annual financial statements produced in accordance with accounting principles? • Is there any unsound accounting manipulation of statements (i.e., figures subject to financial statements and disclosure) such as carrying over of losses that should be realized? • Are the required amounts of write-offs and provisioning determined by self-assessment appropriated in the financial statements? • Are soundness of accounting principles and reliability of financial statements secured through adequate auditing?

E. Contingency Plan

1. Compilation and understanding of a contingency plan

Check points			Specific sample questions
a. Compila-tion of a contingency plan	Has the bank drawn up a countermeasure (contingency plan) against disasters and accidents?		• Has the bank drawn up a comprehensive plan for the head office and all branches, and is there a manual for it? • Is there a section responsible for drawing up and coordinating the plan?
b. Under-standing of the plan	Are the management and the staff aware of the contingency plan, and do they fully understand it?		• Is the management aware of the plan, and do they fully understand it? • Are the staff aware of the plan, and do they fully understand it? • Is the plan approved by the board of directors?
c. Content of the plan	Does the contingency plan enable the bank to continue its operations in case of emergency?	(1) Managerial factors	• Does the plan give due consideration to the safety of customers and employees in case of an emergency? • Does the plan clearly designate an emergency headquarters to be in charge of dealing with a crisis? • Does the plan assess the degree of impact an emergency will have on operations? • Does the plan clearly designate the priority level of each operation, delegation of authority, and arrangements for obtaining the necessary staff in case of an emergency?

			• Does the plan clearly state the order and method of contacting management and staff in case of an emergency? • Does the bank have a means of communication with entities operating payment systems and supervisory authorities, etc., in case of an emergency?
		(2) Material factors	• Does the plan take into consideration electricity, water, and food supply? • Does the plan clearly designate the necessary action to protect assets such as securing a warehouse to store things and deciding the evaluation procedure for damaged property? • Has the bank secured backup data in a vault and/or distant location? • Does the bank have in place a backup center or a backup contract with trustworthy subcontractors or other banks? • Has the bank secured multiple communications methods using private lines between the head office and branches, and between the computer center and branches? • Has the bank secured countermeasures (i.e., alternative office space, etc.) in the event of an emergency (in particular, for overseas branches)?
d. Review and on-site drilling of the plan	Does the bank have a system for reviewing the contingency plan when appropriate, and are on-site drills		• Does the bank have a system to review the plan when necessary? • Are on-site drills conducted regularly at the head office against possible shutdown of the system?

	conducted regularly?	• Are on-site drills conducted regularly at both the head office and branches? • Are results of on-site drills reported to management after appropriate assessment, and utilized in reviewing the plan?

Review Questions:

1. How risk management influence business?
2. Explain the types of business.
3. Describe the scope of risk managers' duties.
4. Explain the risk management corporate policy.
5. Explain the risk management corporate strategy.

*   *   *

UNIT 3

RISK IDENTIFICATION AND MEASUREMENT

Risk identification can be a real learning experience for everyone involved in the identification process and in the organization. Some risks are fairly obvious and others take a little more thought and foresight to fully understand and identify as a truly potential risk. There are several ways that this identification of risk can be achieved. One is by consulting with the various groups within the association to ask them their opinions on certain questions or concerns. Within this consultation process the people asking the questions should be "Very Good" listeners and document the findings of the opinions given. There is an old saying "you would be surprised what you can learn by listening"

By being a good listener, you also do not steer the discussions into the areas or topics that you feel are important. The person being asked the questions provides you with the topics of concern. During this identification phase you should try to ask questions that either probe deeper into the topic or clarify a certain point. There are different sorts of risks and we need to decide on a project by project basis what to do about each type.

Business risks are ongoing risks that are best handled by the business. An example is that if the project cannot meet end of financial year deadline, the business area may need to retain their existing accounting system for another year. The response is likely to be a contingency plan developed by the business, to use the existing system for another year.

Generic risks are risks to all projects. For example the risk that business users might not be available and requirements may be incomplete. Each organization will develop standard responses to generic risks.

Risks should be defined in two parts. The first is the cause of the situation (Vendor not meeting deadline, Business users not available, etc.). The second part is the impact (Budget will be exceeded, Milestones not achieved, etc.). Hence a risk might be defined as "The vendor not meeting deadline will mean that budget will be exceeded". If this format is used, it is easy to remove duplicates, and understand the risk.

Identification Methods

Check list:

Risk Management is an economic operation for a company's assets, liabilities and earnings. Its objective is to minimize uncertainties and contingencies in cash flows from the impact of fortuitous losses arising in the course of the company's operations. It seeks to achieve financial stability through conscious decisions on risk retention and risk transfers. In the matter of risk transfers the decisions involve commercial contracts wherein risks are transferred contractually to vendors, contractors and suppliers or even customers.

Risk Management Completion Checklist

Intended use of this checklist	For a risk management team and/or a Risk Manager to evaluate the effectiveness of the risk management process. The checklist contains items to consider when a project finishes, or when a major phase finishes, to ensure the process works well, that lessons learned have been captured, and that the risk management effort was worth the investment it took.

No.		Items to be considered
1		Was it identified in the Project Plan when the effectiveness of a risk management process would be evaluated? (phase completion, periodically, project completed or terminated)
2		Were review session(s) organized with appropriate people invited to attend?
3		Were the results of the risk management activities reviewed? The results should have included at least the following:
		• Risks that were detected initially and successfully handled
		• Risks that were detected during the project, but not identified at the start

No.		Items to be considered
		• Problems that arose during the project, but were not detected as risks at any point
		• Cost and effort of the risk management activities
		• Cost and effort of risk mitigation activities
		• Cost and effort of contingency plans that were implemented
4		Did the review session identify any implementation problems from the participants?
5		Were any lessons for future risk management processes identified? Items of interest should have included:
		• Mitigation activities that were effective
		• Contingency actions that were successful
		• Changes to the ineffective mitigation activities
6		Were changes identified to risk factors for use in the future? Items of interest should have included:
		• New factors to include in the appropriate risk factor table
		• Factors that can be removed from the table
		• Changes in the cues provided in the chart for high, medium, and low risks
7		Were the results of the analysis incorporated into risk factor tables and the risk management process?
8		Were the results of the analysis disseminated to other projects that were using the risk management process at that time?

Questionnaire

A common place instrument for collecting data beyond the physical reach of the researcher, that is, from a large or diverse sample of people. It is an

impersonal instrument for collecting information and must, therefore, contain clear questions, worded as simply as possible to avoid any confusion or ambiguity since the researcher probably will not be present to explain what was meant by any one particular question.

Risk Management Questionnaire

Model: 1

Date:

Name:

Title/Group:

Location/Telephone:

1. What is the Purpose/Mission/Objective of this work unit?
2. What are the primary strengths of this work unit?
3. What obstacles do you see that affect your goals and objectives?
4. If you had additional resources to help you achieve your objectives, what would they be?
5. What is the worst thing that could happen in your work unit?
6. What is the worst thing that has already happened in your work unit?
7. What are the critical interfaces (other work groups), and which give you the most concern (and why)?

Model:2

Title(s) of Practice(s)

1. (a) Is a written record kept of every business telephone conversation by all Partners and staff?

YES/NO

(b) If no please give details of what method is used

2. (a) Does the Practice have an accounting system, which complies with SAR (Solicitors Accounts Rules)?.

YES/NO

(b) Is this manual or computerized?

MANUAL/COMPUTERISED

(c) Who is authorized to request cheques?

(d) Who is authorized to sign cheques?

(e) Number of signatories?

3. Does the Practice have an e-mail and/or internet user policy or any other formal guidelines for the use of e-mail and/or internet?
YES/NO

If yes, please provide a copy and details of how such guidelines are enforced.

4. (a) Does the Practice always obtain satisfactory written references immediately preceding the engagement of any Employee, Partner or Principal?
YES/NO

If no, please provide details

(b) Are arrangements in place to keep staff up to date with changes in law and procedure?
YES/NO

(c) Do you undertake a conflict search when opening each new file?

YES/NO

5. (a) Do you have an index of cases?
YES/NO

(b) Does the Practice carry out regular audits on all active files?
YES/NO

(c) How many active files are run per fee earner?

(d) How do you supervise staff?

(e) What quality controls are in place?

(f) Is all incoming mail checked by a Partner?
YES/NO

6. Does the Practice operate a centralized or departmental diary system?

YES/NO

If yes, please provide details

7. Do you restrict to Partners those who can give undertakings? **YES/NO**

8. Please attach a copy of:

(a) Your Rule 15 client care letter

(b) Your complaints procedure

9. (a) Has the Practice been subject to 'Intervention' by the Law Society?

YES/NO

(b) Has the Practice or any Employee, Partner or Principal of the Practice been the subject of a Law Society Disciplinary Order in the last 5 years?
YES/NO

10. Is each area of work and are all the branches (if applicable) supervised by a Partner in the Practice?
YES/NO

11. Have you obtained ISO 9000/9001/9002 or Lexcel accreditation?
YES/NO

Have you a Legal Aid Franchise?
YES/NO

Other (please specify)

12. (a) Have you encountered any Date Recognition Compliance problems with your own internal systems or with others' internal systems that you are reliant upon?
YES/NO

If yes, please give details including all measures taken to rectify such problems.

(b) (i) Are you aware of any claims, circumstances or complaints in respect of any advice given in relation to Date Recognition?
YES/NO

(ii) Have you notified SIF or Underwriters of any circumstances likely to give rise to a claim against the Practice in relation to Date Recognition Compliance?
YES/NO

If yes to either (i) or (ii) please give details.

DECLARATION

I / We declare that the statements contained within this supplementary questionnaire are correct to the best of my/our knowledge.

Signed:

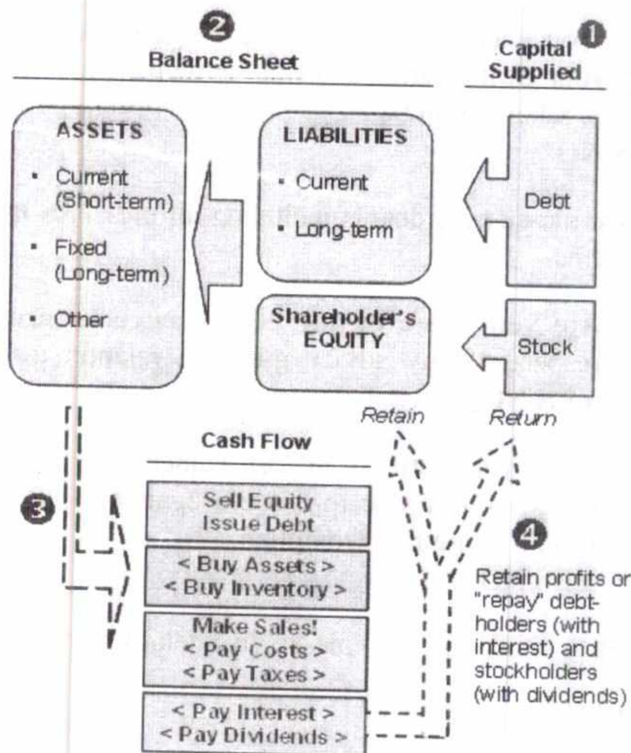
For and on behalf of:

Date:

Financial Statement Analysis

The Financial Statements Are a System (Balance Sheet & Statement of Cash Flow). Financial statements paint a picture of the transactions that flow through a business. Each transaction or exchange--for example, the sale of a product or the use of a rented facility--is a building block that contributes to the whole picture.

Let's approach the financial statements by following a flow of cash-based transactions. In the illustration below, we have numbered four major steps:



1. Shareholders and lenders supply capital (cash) to the company.

2. The capital suppliers have claims on the company. The balance sheet is an updated record of the capital invested in the business. On the right-hand side of the balance sheet, lenders hold liabilities and shareholders hold

equity. The equity claim is "residual", which means shareholders own whatever assets remain after deducting liabilities.

3. The capital is used to buy assets, which are itemized on the left-hand side of the balance sheet. The assets are current, such as inventory, or long-term, such as a manufacturing plant.

4. The assets are deployed to create cash flow in the current year (cash inflows are shown in green, outflows shown in red). Selling equity and issuing debt start the process by raising cash. The company then "puts the cash to use" by purchasing assets in order to create (build or buy) inventory. The inventory helps the company make sales (generate revenue), and most of the revenue is used to pay operating costs, which include salaries.

5. After paying costs (and taxes), the company can do three things with its cash profits. One, it can (or probably must) pay interest on its debt. Two, it can pay dividends to shareholders at its discretion. And three, it can retain or re-invest the remaining profits. The retained profits increase the shareholders' equity account (retained earnings). In theory, these reinvested funds are held for the shareholders' benefit and reflected in a higher share price.

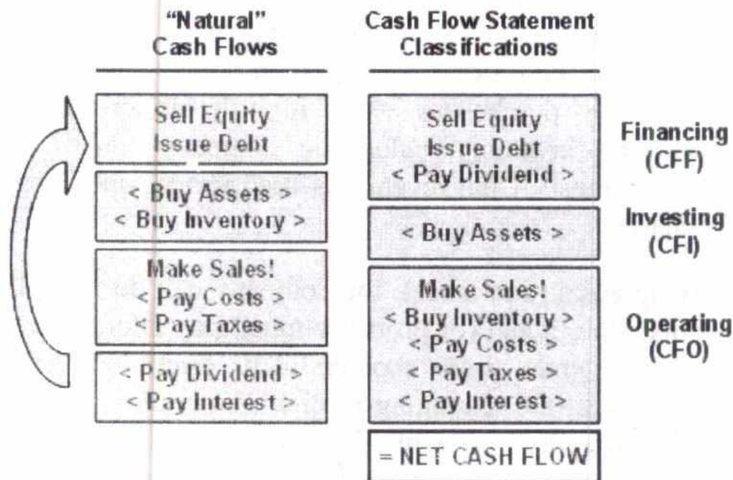
6. This basic flow of cash through the business introduces two financial statements: the balance sheet and the statement of cash flows. It is often said the balance sheet is a static financial snapshot taken at the end of the year (please see "Reading the Balance Sheet" for more details), whereas the statement of cash flows captures the "dynamic flows" of cash over the period (see "What is a Cash Flow Statement?").

Statement of Cash Flows

The statement of cash flows may be the most intuitive of all statements. We have already shown that, in basic terms, a company raises capital in order to buy assets that generate a profit. The statement of cash flows "follows the cash" according to these three core activities: (1) cash is raised from the capital suppliers (which is the 'cash flow from financing', or CFF), (2) cash is used to

buy assets ('cash flow from investing', or CFI), and (3) cash is used to create a profit ('cash flow from operations', or CFO).

However, for better or worse, the technical classifications of some cash flows are not intuitive. Below we recast the "natural" order of cash flows into their technical classifications:



You can see the statement of cash flows breaks into three sections:

1. Cash flow from financing (CFF) includes cash received (inflow) for the issuance of debt and equity. As expected, CFF is reduced by dividends paid (outflow).

2. Cash flow from investing (CFI) is usually negative because the biggest portion is the expenditure (outflow) for the purchase of long-term assets such as plants or machinery. But it can include cash received from separate (that is, not consolidated) investments or joint ventures. Finally, it can include the one-time cash inflows/outflows due to acquisitions and divestitures.

3. Cash flow from operations (CFO) naturally includes cash collected for sales and cash spent to generate sales. This includes operating expenses

such as salaries, rent and taxes. But notice two additional items that reduce CFO: cash paid for inventory and interest paid on debt.

The total of the three sections of the cash flow statement equals net cash flow: CFF + CFI + CFO = net cash flow. We might be tempted to use net cash flow as a performance measure, but the main problem is that it includes financing flows. Specifically, it could be abnormally high simply because the company issued debt to raise cash, or abnormally low because it spent cash in order to retire debt.

CFO by itself is a good but imperfect performance measure. Consider just one of the problems with CFO caused by the unnatural re-classification illustrated above. Notice that interest paid on debt (interest expense) is separated from dividends paid: interest paid reduces CFO but dividends paid reduce CFF. Both repay suppliers of capital, but the cash flow statement separates them. As such, because dividends are not reflected in CFO, a company can boost CFO simply by issuing new stock in order to retire old debt. If all other things are equal, this equity-for-debt swap would boost CFO.

FINANCIAL STATEMENT ANALYSIS

Provides information on financial statement analysis especially drawing ratio analysis to explain financial circumstances.

Ratio Analysis

A financial ratio helps investors in analysis of financial health of the company and forms the basis on which investments are planned. Lets look at some of the widely used rations for analysis of various aspects related to financial health of the company.

1. Current Ratio

Current Ratio tells us the current financial strength of the company, primarily in terms of the cash and credit standing of the company. It answers

questions like 'Is the company spending too much or is it holding too much cash back?

Current Ratio = Current Assets / Current Liabilities

2. Debt to Equity Ratio

Debt to Equity ratio tells us the amount of debt of the company against the shareholders equity

Debt to Equity ratio = Total Liabilities / Total Shareholders Equity

3. Asset Turnover Ratio

The ratio tells us the kind of revenue that is generated using the total assets of the company It is an indicator on performance of the assets, whether they under performing or over performing.

Asset Turnover Ratio = Sales / Average Total Assets

4. Interest Coverage Ratio

The ratio tells us the amount of earnings that company holds to make interest payments of its debt.

Interest Coverage ratio = Income Before Interest and Income Tax Expenses / Interest Expense

5. Inventory Turn Ratio

The ratio tells us how many times a business turns its inventory over a period of time. It indicates if the company has most of its assets tied up in inventory and if they are under performing.

Inventory Turnover Ratio = Cost of Goods Sold / Average Inventories

6. Operating Profit Margin Ratio

The ratio tells us the operating efficiency of the company. The percentage of profit it makes after deduction of its operating expenses.

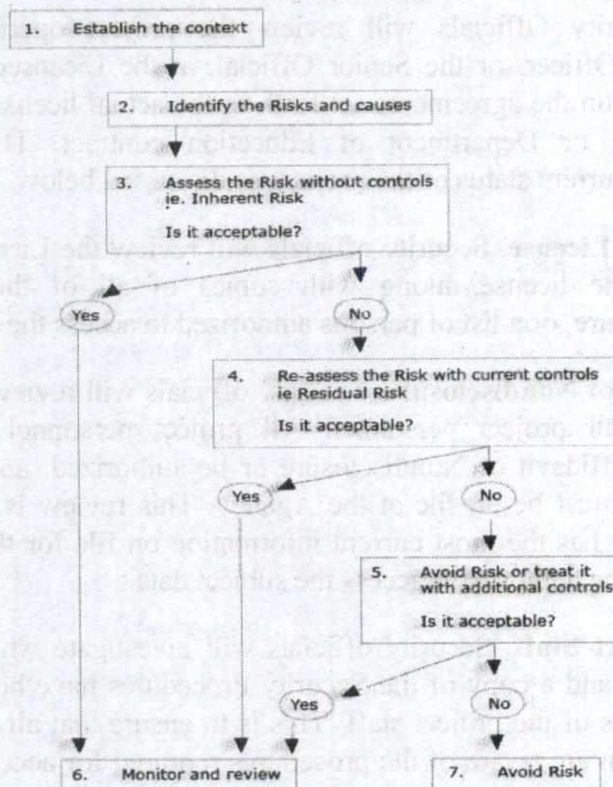
Operating Profit Margin Ratio = Net Income – Operating Expenses / Total Sales

7. Quick Test Ratio

Investors widely use the Quick Test Ratio to arrive at the liquidity strength of the company and its overall financial standing.

Quick ratio = Quick Assets / Current Liabilities

Risk Management Flow chart:



ON-SITE INSPECTION
On-Site Inspection Procedures

Under the provisions of the license, the Agency may conduct **unannounced** and **unscheduled** inspections of the license site to assess compliance with the terms of the license.

Specifically, security officials will visit the Licensee's facilities to evaluate compliance in the following two areas, which are explained in detail in this section:

- Operational Procedures
- Security Procedures and Security Plan

License Procedures

Data Security Officials will review the project operations with the Principal Project Officer, or the Senior Official, at the Licensee's facility. This review will focus on the agreements set forth in the actual license, memorandum of understanding, or Department of Education contract. This includes an inspection of the current status of the project, as discussed below.

- **Record of License.** Security officials will review the Licensee's file for a copy of the license, along with copies of all of the Affidavits of Nondisclosure, or a list of persons authorized to access the data.

- **Affidavits of Nondisclosure.** Security officials will review the names and status of all project personnel. All project personnel must have an executed Affidavit of Nondisclosure or be authorized, and these original Affidavits must be on file at the Agency. This review is to confirm that the Agency has the most current information on file for those individuals who have the authority to access the subject data.

- **The Project Staff.** Security officials will investigate whether a copy of the license and a copy of the Security Procedures have been reviewed by all members of the project staff. This is to ensure that all members of the project team are aware of the procedures required for accessing restricted-use data.

Security Procedures and Security Plan

Security officials will review with the Licensee all aspects of the Licensee's security procedures for the restricted data. These procedures are documented in the Security Procedures, which are included in the licensing package.

Security officials will also review the Licensee's submitted Security Plan, which is the on-site implementation document for the Security Procedures.

Security officials will review these procedures for compliance. A basic outline of these procedures, in the form of the **On-Site Inspection Guideline.**

Record of Losses

The main concern of risk to property and people is record of losses. Some examples of losses include:

1. LOSS BY DESTRUCTION – Property may be destroyed by fire, earthquake, flood, wind, breakage, or deterioration.

2. LOSS BY CONFISCATION - Property may be confiscated by an act of crime such as theft, embezzlement, robbery, burglary, forgery, and conversion.

3. LOSS OF USE - When property is destroyed or confiscated, the loss is often increased because of the indirect loss, e.g., loss of income, interruption of activities and extra expenses to continue operations. Much greater than the loss to physical property, is the loss of records and data which are vital to the operation of the University.

4. LOSS BY NEGLIGENCE - Liability claims are incurred when persons are injured or property of others is damaged or destroyed due to negligence.

5. LOSS OF EMPLOYEE/STUDENTS GOODWILL - Discrimination, sexual harassment, libel, slander, bad faith and unfair dealings will create liability situations and poor employee/student and public relations issues.

Threat Analysis

The first stage of a threat analysis in project risk management is to identify threats facing you. Threats may be:

- **Human** - from individuals or organizations, illness, death, etc.
- **Operational** - from disruption to supplies and operations, loss of access to essential assets, failures in distribution, etc.
- **Reputational** - from loss of business partner or employee confidence, or damage to reputation in the market.
- **Procedural** - from failures of accountability, internal systems and controls, organization, fraud, etc.
- **Project** - risks of cost over-runs, jobs taking too long, of insufficient product or service quality, etc.
- **Financial** - from business failure, stock market, interest rates, unemployment, etc.
- **Technical** - from advances in technology, technical failure, etc.
- **Natural** - threats from weather, natural disaster, accident, disease, etc.
- **Political** - from changes in tax regimes, public opinion, government policy, foreign influence, etc.

This analysis of threat is important because it is so easy to overlook important threats. One way of trying to capture them all is to use a number of different approaches:

- Firstly, run through a list such as the one above, to see if any apply
- Secondly, think through the systems, organizations or structures you operate, and analyze risks to any part of those
- See if you can see any vulnerabilities within these systems or structures
- Ask other people, who might have different perspectives.

Once you have identified the threats you face, the next step is to work out the likelihood of the threat being realized and to assess its impact.

One approach to this is to make your best estimate of the probability of the event occurring, and to multiply this by the amount it will cost you to set things right if it happens. This gives you a value for the risk.

Once you have worked out the value of risks you face, you can start to look at ways of managing them. When you are doing this, it is important to choose cost effective approaches - in most cases, there is no point in spending more to eliminating a risk than the cost of the event if it occurs. Often, it may be better to accept the risk than to use excessive resources to eliminate it.

Risk may be managed in a number of ways:

- **By using existing assets:**

  Here existing resources can be used to counter risk. This may involve improvements to existing methods and systems, changes in responsibilities, improvements to accountability and internal controls, etc.

- **By contingency planning:**

  You may decide to accept a risk, but choose to develop a plan to minimize its effects. A good contingency plan will allow you to take action immediately, with the minimum of project control.

- **By investing in new resources:**

  Your risk analysis should give you the basis for deciding whether to bring in additional resources to counter the risk. This can also include insuring the risk: Here you pay someone else to carry part of the risk - this is particularly important where the risk is so great as to threaten your or your organization's solvency.

Once you have carried out a risk analysis and management exercise, it may be worth carrying out regular reviews. These might involve formal reviews of the risk analysis, or may involve testing systems and plans appropriately.

Event analysis

Event analysis is an umbrella terms for a set of procedures. As such it is a specialized subfield of time series analysis which uses techniques, such as Poisson regression, which are designed to analyze rare events (time series in

which most data are non-events). It is prominent in the field of international relations, where it has been used to analyze time series of international conflict and diplomatic events related to project and risk management. It is also used in biostatistics, in the study of demographic changes, and a variety of other fields.

Event analysis can be a form of panel study in which the periods of observation are not arbitrarily spaced but instead measurement is taken at each stage of a sequence of events. The timing and spacing of observations thus becomes a critical variable in its own right. Moreover, often in event analysis studies the data may not be interviews of individuals as in panel studies, but rather measurements pertaining to organizations or even governments.

Safety Audit

Safety audits examine and assess in detail the standards of facets of a particular activity. They extend from complex technical operations and emergency procedures to job descriptions and attitudes.

Safety audits provide increased assurance that facilities are being operated and maintained in a way that properly protects the safety and health of the employees, the environment, the surrounding community, plant assets and continuity of operations.

These audits cover items such as:

- Correct materials of construction
- Correct codes, standards and engineering practices
- Operating and maintenance procedures

Measurement Methods

Frequency and severity measures

The benefits of measuring and streamlining the flow of capital, people and information into and out of the enterprise were realized long ago outside the financial sector, as evidenced by the management programmes Total Quality Management, Six Sigma and Shareholder Value Added introduced at companies like US conglomerate General Electric and communications firm Motorola.

With the search for value by customers and shareholders, deregulation and global competition transforming the financial services industry, there should be no need to wait for the Basle Committee to claim its operational risk claw-back before acting.

Of course, quantifying operational risk is a challenge, if it means supporting enterprise-wide performance measurement and capital allocation. But this is not the only possible objective. Simpler models, delivering relative or subjective measures – risk indicators, ratings, or impact measures – are widely used already. These are intended to:

- Improve the quality of workflow;
- Reduce losses caused by process failure;
- Change risk culture; and
- Provide early warning of deterioration in systems or management.

Most of the major publicized losses at financial institutions of the past few years were due wholly or partly to operational risk, for example, the losses sustained last year by investors in hedge fund Long-Term Capital Management, and by Sumitomo, Daiwa, NatWest and Barings. In such cases it seems far-fetched to suppose that quantification and risk capital attribution alone can help. For such low-frequency, high-impact events as rogue trader syndrome, internal data will probably never be statistically valid.

The current tendency among modellers is to look outside the enterprise and 'fit' external data from comparable organisations. By this means, one could attempt to set aside enough risk capital to ride out the rogue trader event, if it were to occur.

But then the business line's returns and competitiveness in the market are tied to that of the organisations used for benchmarking, leaving no incentive for investment in the kind of management controls that might have prevented or tempered the event in the first place. The lesson is that statistical models based on external data must be leavened with some form of internal "marking-to-operations".

Operational risk can be divided into operational leverage risk (also known as business or strategic risk) and operational failure risk. Operational leverage risk is the risk that the organisation's operations will not generate the expected returns as a result of external factors, such as changes in the tax regime, in the political, regulatory or legal environment, or in the nature or behaviour of the competition.

Modelling this kind of risk is best carried out using scenario analysis. Operational failure risk is the risk that losses will be sustained, or earnings foregone, as a result of failures in processes, information systems or people. In contrast to leverage risk, the risk factors in failure risk are primarily internal.

Modeling Losses

In the sections that follow, we show how to combine distributional assumptions for event frequency and severity to derive loss estimates, using the familiar example of transaction processing errors.

Although it would be possible to model total transaction handling losses as a single distribution, it is preferable to combine separate distributions for the mishandling event process and the severity. This has a number of advantages. These include better drill-down into the causes and effects of losses, and the improved ability to set trigger thresholds for implementing dynamic control processes as part of the workflow and to see the effects of those controls.

The event process for transaction handling errors is best approximated as a poisson process, in which the frequency of error events per unit of time is distributed as a poisson variable (although in theory, the exponential distribution could also be used to model the distribution of the time between errors).

Probability Approach

Risk is a combination of the probability of a negative event and its consequences. If an event is inevitable but inconsequential, it does not represent a risk, because it has no impact. Alternatively, an improbable event with significant consequences may not be a high risk. These two factors are combined in what we experience as the possibility of loss, failure, danger, or peril.

$$\text{Project Risk} = \sum (\text{Events} * \text{Probabilities} * \text{Consequences})$$

An easy way to reduce risk is to have less ambitious goals. After evaluating risks, one can choose a path of risk avoidance or risk mitigation and management. If we understand the risks on a project, we can decide which risks are acceptable and take actions to mitigate or forestall those risks. If our project risk assessment determines risks are excessive, we may want to consider restructuring the project to within acceptable levels of risk.

Risks that do not offer the potential for gain (profit?)should be avoided. Risks associated with achieving challenging and worthwhile goals should be managed. One way to reduce risk is to gather information about relevant issues to lower the level of uncertainty. Then we can look for ways to reduce probabilities of failures or to reduce their consequences.

What may look like an unacceptable risk to one person might rightly appear as an attractive opportunity to another. The difference is vision.

Items in the project plan that are important and that are uncertain of success should be considered risk areas and given special attention. Risk should be associated with areas where the scope is not well defined or is subject to change. An unproven or immature technical approach, or known technical difficulty or complexity will increase project risk. Ambitious goals always result in risk. Unfamiliarity with the process, or inexperienced personnel, constitute project risks, if for no other reason than being unknowns. Exterior interfaces cause risks because they can change and, even if they don't change, their descriptions or specifications may be inaccurate. Exterior organizational dependencies create project risks. Incomplete planning or optimistic cost or schedule goals create risk. If the customer is involved in schedule dependencies for document review and approval or for delivering process information, this creates project risks. Conversely, project risks are created if the customer is not involved in periodic review of the system design and project plans.

Any area over which the project manager does not have control can be project risks. Anything that is not well understood, anything that is not well

documented, and anything that can change, these all create project risks. Things that haven't been tested are always at risk.

An organizational culture that has previously had problems executing projects will be likely to repeat the same mistakes. These problem areas should be understood and managed as significant project risks. They must be counteracted by specific bold mitigating management initiatives or repeated failures are guaranteed

The known unknowns are more likely to be project risks than the unknown unknowns. This means you should trust your instincts and pay attention to what seems risky to you. It is more likely you will have problems from known risk areas than be surprised by things completely unforeseen.

Risk analysis consists of risk identification, probability assessment, and impact estimate. Start by identifying all the risk events that can occur on your project. Then estimate the probability of each event happening. Finally, estimate the impact in hours or dollars if the event occurs.

Once you have listed and quantified the project risks, then you should prepare a risk management plan for each significant risk item. The final step would be to formalize this into a risk management activity, establish metrics, and track your top ten risks week by week.

Risk Event	*Probability*	*Impact*	*Risk Score*	*Risk Mitigation Plan*
Change host operating system	.2	100 hours	20 hours	Work with host support group
Redesign data model	.4	200 hours	80 hours	Do early prototyping
Data conversion is late	.7	300 hours	210 hours	Request tracking of progress
Total Risk:			310 hours	

Schedule Risk Assessment using PERT

PERT is an acronym for Program Evaluation and Review Technique. A PERT chart is a Critical Path Method (CPM) chart considered statistically. It can be useful in assessing schedule risk, and schedule risk usually turns into cost risk. ((I have never actually seen this used on a project.))

The essential nature of PERT analysis is to determine the expected time for each activity by using a weighted average of the most likely along with the best case and worst case time estimate that can reasonably be imagined. The normal approach to PERT is to weights the "most likely" four times heavier than the extremes, then sum them all and divide by six. When the expected times have been determined for all activities on the critical path, these can be summed to determine the expected time for the entire project.

The standard deviation can be determined for each element in the network using the formula (b-a)/6. The standard deviation for the entire project will be the square root of the sum of the squares of the standard deviations of the individual elements. Having the standard deviation for the total project, one can then assess the probability of different schedule outcomes.

If the standard deviation for a total project is one month, you can consult a Standard Normal Distribution table to see that one standard deviation includes 84% of the population. Therefore, the probability that the project will complete no more than one month late is 84%. The probability that it will complete at least one month early is 1-84% or 16%. You can use the standard deviation for the total project to evaluate probabilities for different outcomes by converting a completion date to standard deviations from the expected time and then using the table to find the probability of occurrence.

While this is an interesting concept, it is only used in practice for projects with often repeated tasks and highly standardized methodologies. In all other projects, there are so many other unknowns, uncertainties, and instabilities that PERT analysis is insensitive to all the most relevant issues driving the schedule risk. In other words, it may be pointless to do statistical analysis if you already understand where your problems are.

Review Questions:

1. How to identify risk?
2. Describe the risk measurement techniques.
3. What is checklist?
4. Define questionnaire.
5. What is financial statement analysis?
6. Explain a flowchart.
7. What is onsite inspection?
8. Define threat analysis.
9. What is event analysis?
10. What is safety audit?
11. Describe frequency and severity measures of risk.
12. Explain the probability approach for risk measurement

* * *

UNIT 4

RISK EXPOSURE LOSSES

Risk Exposure is a simple calculation that gives a numeric value to a risk, enabling different risks to be compared.

Risk Exposure of any given risk =
Probability of risk occurring x total loss if risk occurs

A limitation of this calculation is that it will give the same scores to high-probability/low loss risks and low-probability/high loss risks. If you are concerned with these differences, a Risk Matrix may be a better way of evaluating risks.

Property Loss Exposure

- Replacement or repair of vehicles, buildings, machinery, raw materials, goods in process and finished goods subject to physical and human perils on the premises or in transit.
- Shutdown or slowdown of operations because of property losses.
- Accidental breakdown of electrical or mechanical equipment, air conditioning, refrigeration, boilers, pressure vessels, and production and processing equipment

TYPES

Liability Losses

- Liability for bodily injury or property damage to 1) third parties because of defective products, 2) visitors because of hazards on premises, and 3) others because of your operations.
- Legal responsibility due to the workers' compensation laws for bodily injuries to employees.

Personal Losses

- Automobile accidents.

- Losses because of the death or disability of employees.
- Losses to families of employees because of death, poor health or retirement of employees.

Net Income Loss Exposure

Types of Loss Exposures within the province of risk management include:

- Property - Real & Personnel, Tangible & Intangible
- Net Income - Reduction in Revenue or Increase in Expense; can be due to loss of Property (yours or suppliers, or customers) or loss due to Civil or Statutory fines and judgments, or by loss of Key Personnel
- Liability - Civil and Statutory (Torts, Statutory Workers Compensation, EPA and other Administrative laws)
- Personnel - Through Death, Disability, or Retirement Key Personnel or catastrophic loss to many employees

Risk management strategies involve many concepts. Some of them include the following concerns:

Elements of Loss Expense

- Actual damages to physical assets to repair or replace.
- Increase in expenses or reduction of revenue due to loss.
- Cost of investigation, legal fees, fines and awarded judgments.
- Loss of worker productivity and adverse publicity and public opinion.
- Higher potential insurance premiums.
- Payments made due to the death, disability or resignation of employees.

Risk Control Techniques

- Avoidance of activities which cause loss.
- Reduction of the frequency of loss - risk prevention.
- Reduction of the severity of loss - risk reduction.
- Contractual transfer of responsibility for loss occurrence.

Risk Financing Techniques

- Retention of losses either by design or omission or by an owned captive insurance company.
- Borrowing of funds or use of bonds etc.
- Contractual non-insurance transfer of responsibility for loss payment.
- Insurance transfer to a non-owned insurance company when and if the exposure is insurable and the cost is not prohibitive.

Risk management is concerned with all loss exposures, not only the ones that can be insured. Insurance is a technique to finance some loss exposures and, therefore, a part of the broader concept of managing risk; not the other way around.

Elements of Loss Expense

- Actual damages to physical assets to repair or replace.
- Increase in expenses or reduction of revenue due to loss.
- Cost of investigation, legal fees, fines and awarded judgments.
- Loss of worker productivity and adverse publicity and public opinion.
- Higher potential insurance premiums.
- Payments made due to the death, disability or resignation of employees.

Valuation of Potential Loss

The risk management task of identifying and valuing potential loss exposures. The value assigned to each risk may be based on replacement cost, actual cash value (physical depreciation considered), and original cost, depreciated value, market value, or tax appraised value, depending on its current use and the organization's financial structure. Once loss exposures are identified and valued, funding for a potential loss, including transfer of risk, can be developed.

In project management, risk management includes the following activities:

- Planning how risk management will be held in the particular project. Plan should include risk management tasks, responsibilities, activities and budget.

- Assigning risk officer - a team member other than a project manager who is responsible for foreseeing potential project problems. Typical characteristic of risk officer is a healthy skepticism.

- Maintaining live project risk database. Each risk should have the following attributes: opening date, title, short description, probability and importance. Optionally risk can have assigned person responsible for its resolution and date till then risk still can be resolved.

- Creating anonymous risk reporting channel. Each team member should have possibility to report risk that he foresees in the project.

- Preparing mitigation plans for risks that are chosen to be mitigated. The purpose of the mitigation plan is to describe how this particular risk will be handled – what, when, by who and how will be done to avoid it or minimize consequences if it becomes a liability.

- Summarizing planned and faced risks, effectiveness of mitigation activities and effort spend for the risk management.

Civil Liabilities of Business Houses

Form contracts

Among legal commentators, standard form contracts have long been received with distrust, and the rules governing their interpretation have engendered considerable controversy. While economic analysis has little to say regarding the libertarian objection to standard form contracts or their relationship to personal autonomy, it can help evaluate their effects on efficiency and the distribution of the gains from trade. From such a perspective, standard forms should be analyzed like any other productive input, comparable to design, marketing, and technical support. Whether their use raises any special regulatory or policy concerns, therefore, depends on their implications for the standard litany of market failures: scale economies, monopoly, externalitics, imperfect information, and the like.

Bankruptcy

Bankruptcy is a legally declared inability or impairment of ability of an individual or organization to pay their creditors. A declared state of bankruptcy can be requested or initiated by the bankrupt individual or organization, or it can be requested by creditors in an effort to recoup a portion of what they are owed. However, in the overwhelming majority of cases, the bankruptcy is initiated by the "bankrupt" individual or organization.

Person selected by a judge or creditors of a bankrupt individual to handle matters including the sale of the bankrupt's assets, management of the funds from the sale of those assets, payment of expenses, and distribution of the balance to creditors. The trustee is usually compensated with a specified percentage of the liquidation sale.

Review Questions:

1. What is property loss exposure?
2. What is net income loss exposure?
3. What is liability loss exposure?
4. Explain the civil liabilities of business firms.
5. What is a contract?
6. What is bankruptcy?

UNIT 5

RISK MANAGEMENT TECHNIQUES

Investment planning is almost impossible without a thorough understanding of risk. There is a risk/return trade-off. That is, the greater risk accepted, the greater must be the potential return as reward for committing one's funds to an uncertain outcome. Generally, as the level of risk rises, the rate of return should also rise, and vice versa. Before we discuss risk in detail, we should first explain that risk can be perceived, defined and handled in a multitude of ways. One way to handle risk is to avoid it. Risk avoidance occurs when one chooses to completely avoid the activity the risk is associated with. An example would be the risk of being injured while driving an automobile. By choosing not to drive a person could avoid that risk altogether. Obviously, life presents some risks that cannot be avoided. One may view a risk in eating food that might be toxic. Complete avoidance, by refusing to eat at all, would create the inevitable outcome of death, so in this case, avoidance is not a viable choice. In the investment world, avoidance of some risk is deemed to be possible through the act of investing in "risk-free" investments. Short-term maturity United States government bonds are usually equated with a "risk-free" rate of return. Stock market risk can be completely avoided by one choosing to have no exposure to it by not investing in equity securities.

Risk Transfer

Another way to handle risk is to transfer the risk. An easy to understand example of risk transfer is the concept of insurance. If one has the risk of becoming severely ill (and unfortunately we all do), then health insurance is advisable. An insurance company will allow you to transfer the risk of large medical bills to them in exchange for a fee called an insurance premium. The company knows that statistically, if they collect enough premiums and have a large enough pool of insured, they can pay the costs of the minority who will require extensive medical treatment and have enough left over to record a profit. Risk transfer can also occur in investing. One may choose to purchase a municipal bond that is insured. One may purchase a put option on a stock which allows that person to "put to" or sell to someone their stock at a set price,

regardless of how much lower the stock may drop. There are many examples of risk transfer in the area of investing.

The Risk Adverse Investor

Do investors dislike risk? In economics in general, and investments in particular, the standard assumption is that investors are rational. Rational investors prefer certainty to uncertainty. It is easy to say that investors dislike risk, but more precisely, we should say that investors are risk averse. A risk-averse investor is one who will not assume risk simply for its own sake and will not incur any given level of risk unless there is an expectation of adequate compensation for having done so. Note carefully that it is not irrational to assume risk, even very large risk, as long as we expect to be compensated for it. In fact, investors cannot reasonably expect to earn larger returns without assuming larger risks.

Investors deal with risk by choosing (implicitly or explicitly) the amount of risk they are willing to incur. Some investors choose to incur high levels of risk with the expectation of high levels of return. Other investors are unwilling to assume much risk, and they should not expect to earn large returns.

We have said that investors would like to maximize their returns. Can we also say that investors, in general, will choose to minimize their risks? No! The reason is that there are costs to minimizing the risk, specifically a lower expected return. Taken to its logical conclusion, the minimization of risk would result in everyone holding risk-free assets such as savings accounts and Treasury bills. Thus, we need to think in terms of the expected return/risk trade-off that results from the direct relationship between the risk and the expected return of an investment.

Influence of Time on Risk

Investors need to think about the time period involved in their investment plans. The objectives being pursued may require a policy statement that speaks to specific planning horizons. In the case of an individual investor this could be a year or two in anticipation of a down payment on a home purchase or a lifetime if planning for retirement. Generally speaking, the longer the time horizon the more risk can be incorporated into the financial planning.

The U.S. Department of Labor, Pension and Welfare Benefits Administration states that since 1926, the average annual return of short-term U.S, Treasury bills, which roughly equals the return of other cash equivalents such as saving accounts, has been 3.8 percent. The annual return of long-term government bonds over the same period has been 5.3 percent. Large-company stocks, on the other hand, have averaged an annual return of 11.2 percent. With these statistics available why wouldn't everyone at all times be 100 percent invested in stocks? The answer is, of course, that while over the long term stocks have outperformed, there have been many short term periods in which they have under-performed, and in fact, have had negative returns. Exactly when short term periods of underperformance will occur is unknown and thus there is more risk in owning stocks if one has a short term horizon than if there exists a long term horizon.

Time has a different effect when analyzing the risk of owning fixed income securities, such as bonds. There is more risk associated with holding a bond long term than short term because of the uncertainty of future inflation and interest rate levels. If one were to "lock in" a rate of 6 percent for a bond that matured in one year, an upward move in inflation or interest rates would have a less adverse effect on the price of that bond than a 6 percent bond that matured in thirty years. That is because the bond could be redeemed in one year and reinvested in a bond with a presumably higher interest rate. The thirty year bond, however, will continue to pay only 6 percent for the rest of its thirty year life. More about bond pricing and relationships to interest rates in a future chapter.

A. TYPES OF INVESTMENT RISK

(i) Systematic versus Unsystematic Risk

Modern investment analysis categorizes the traditional sources of risk causing variability in returns into two general types: those that are pervasive in nature, such as market risk or interest rate risk, and those that are specific to a particular security issue, such as business or financial risk. Therefore, we must consider these two categories of total risk. The following discussion introduces these terms. Dividing total risk into its two components, a general (market) component and a specific (issuer) component, we have systematic risk and nonsystematic risk, which are additive:

Total risk = General risk + Specific risk

= Market risk + Issuer risk

= Systematic risk + Nonsystematic risk

Systematic Risk:

An investor can construct a diversified portfolio and eliminate part of the total risk, the diversifiable or nonmarket part. What is left is the nondiversifiable portion or the market risk. Variability in a security's total returns that is directly associated with overall movements in the general market or economy is called **systematic (market) risk**.

Virtually all securities have some systematic risk, whether bonds or stocks, because systematic risk directly encompasses interest rate, market, and inflation risks. The investor cannot escape this part of the risk because no matter how well he or she diversifies, the risk of the overall market cannot be avoided. If the stock market declines sharply, most stocks will be adversely affected; if it rises strongly, as in the last few months of 1982, most stocks will appreciate in value. These movements occur regardless of what any single investor does. Clearly, market risk is critical to all investors.

Nonsystematic Risk:

The variability in a security's total returns not related to overall market variability is called the **nonsystematic (non-market) risk**. This risk is unique to a particular security and is associated with such factors as business and financial risk as well as liquidity risk. Although all securities tend to have some nonsystematic risk, it is generally connected with common stocks.

Remember the difference: Systematic (Market) Risk is attributable to broad macro factors affecting all securities. Nonsystematic (Non-Market) Risk is attributable to factors unique to a security.

(ii) Market Risk

The variability in a security's returns resulting from fluctuations in the aggregate market is known as market risk. All securities are exposed to market risk including recessions, wars, structural changes in the economy, tax law

changes, even changes in consumer preferences. Market risk is sometimes used synonymously with systematic risk.

(iii) Interest Rate Risk

The variability in a security's return resulting from changes in the level of interest rates is referred to as interest rate risk. Such changes generally affect securities inversely; that is, other things being equal, security prices move inversely to interest rates. The reason for this movement is tied up with the valuation of securities. Interest rate risk affects bonds more directly than common stocks and is a major risk faced by all bondholders. As interest rates change, bond prices change in the opposite direction.

(iv) Purchasing Power Risk

A factor affecting all securities is purchasing power risk also known as inflation risk. This is the chance that the purchasing power of invested dollars will decline. With uncertain inflation, the real (inflation-adjusted) return involves risk even if the nominal return is safe (e.g., a Treasury bond). This risk is related to interest rate risk, since interest rates generally rise as inflation increases, because lenders demand additional inflation premiums to compensate for the loss of purchasing power.

(v) Regulation Risk

Some investments can be relatively attractive to other investments because of certain regulations or tax laws that give them an advantage of some kind. Municipal bonds, for example pay interest that is exempt from local, state and federal taxation. As a result of that special tax exemption, municipals can price bonds to yield a lower interest rate since the net after-tax yield may still make them attractive to investors. The risk of a regulatory change that could adversely affect the stature of an investment is a real danger. In 1987, tax law changes dramatically lessened the attractiveness of many existing limited partnerships that relied upon special tax considerations as part of their total return. Prices for many limited partnerships tumbled when investors were left with different securities, in effect, than what they originally bargained for. To make matters worse, there was not an extensive secondary market for these

illiquid securities and many investors found themselves unable to sell those securities at anything but "firesale" prices if at all.

(vi) Business Risk

The risk of doing business in a particular industry or environment is called business risk. For example, as one of the largest steel producers, U.S. Steel faces unique problems. Similarly, General Motors faces unique problems as a result of such developments as the global oil situation and Japanese imports.

(vii) Reinvestment Risk

It is important to understand that YTM is a promised yield, because investors earn the indicated yield only if the bond is held to maturity and the coupons are reinvested at the calculated YTM (yield to maturity).

Obviously, no trading can be done for a particular bond if the YTM is to be earned. The investor simply buys and holds. What is not so obvious to many investors, however, is the reinvestment implications of the YTM measure. Because of the importance of the reinvestment rate, we consider it in more detail by analyzing the reinvestment risk.

Reinvestment Risk: The YTM calculation assumes that the investor reinvests all coupons received from a bond at a rate equal to the computed YTM on that bond, thereby earning interest on interest over the life of the bond at the computed YTM rate. In effect, this calculation assumes that the reinvestment rate is the yield to maturity.

If the investor spends the coupons, or reinvests them at a rate different from the assumed reinvestment rate of 10 percent, the realized yield that will actually be earned at the termination of the investment in the bond will differ from the promised YTM. And, in fact, coupons almost always will be reinvested at rates higher or lower than the computed YTM, resulting in a realized yield that differs from the promised yield. This gives rise to **reinvestment rate risk**.

This interest-on-interest concept significantly affects the potential total dollar return. The exact impact is a function of coupon and time to maturity, with

reinvestment becoming more important as either coupon or time to maturity, or both, rises. Specifically:

a. Holding everything else constant, the longer the maturity of a bond, the greater the reinvestment risk.

b. Holding everything else constant, the higher the coupon rate, the greater the dependence of the total dollar return from the bond on the reinvestment of the coupon payments.

Let's look at realized yields under different assumed reinvestment rates for a 10 percent non-callable 20-year bond purchased at face value. If the reinvestment rate exactly equals the YTM of 10 percent, the investor would realize a 10 percent compound return when the bond is held to maturity, with $4,040 of the total dollar return from the bond attributable to interest on interest. At a 12 percent reinvestment rate, the investor would realize a 11.14 percent compound return, with almost 75 percent of the total return coming from interest on interest ($5,738/ $7,738). With no reinvestment of coupons (spending them as received), the investor would achieve only a 5.57 percent return. In all cases, the bond is held to maturity.

Clearly, the reinvestment portion of the YTM concept is critical. In fact, for long- term bonds the interest-on-interest component of the total realized yield may account for more than three-fourths of the bond's total dollar return.

(viii) International Risk

International Risk can include both Country risk and Exchange Rate risk.

Exchange Rate Risk: All investors who invest internationally in today's increasingly global investment arena face the prospect of uncertainty in the returns after they convert the foreign gains back to their own currency. Unlike the past when most U.S. investors ignored international investing alternatives, investors today must recognize and understand **exchange rate risk**, which can be defined as the variability in returns on securities caused by currency fluctuations. Exchange rate risk is sometimes called *currency risk*.

For example, a U.S. investor who buys a German stock denominated in marks must ultimately convert the returns from this stock back to dollars. If the exchange rate has moved against the investor, losses from these exchange rate movements can partially or totally negate the original return earned.

Obviously, U.S. investors who invest only in U.S. stocks on U.S. markets do not face this risk, but in today's global environment where investors increasingly consider alternatives from other countries, this factor has become important. Currency risk affects international mutual funds, global mutual funds, closed-end single country funds, American Depository Receipts, foreign stocks, and foreign bonds.

Country Risk: Country risk, also referred to as political risk, is an important risk for investors today. With more investors investing internationally, both directly and indirectly, the political, and therefore economic, stability and viability of a country's economy need to be considered. The United States has the lowest country risk, and other countries can be judged on a relative basis using the United States as a benchmark. Examples of countries that needed careful monitoring in the 1990s because of country risk included the former Soviet Union and Yugoslavia, China, Hong Kong, and South Africa.

(ix) Liquidity Risk

Liquidity risk is the risk associated with the particular secondary market in which a security trades. An investment that can be bought or sold quickly and without significant price concession is considered liquid. The more uncertainty about the time element and the price concession, the greater the liquidity risk. A Treasury bill has little or no liquidity risk, whereas a small OTC stock may have substantial liquidity risk.

B. MEASUREMENT OF RISK

(i) Volatility

Of all the ways to describe risk, the simplest and possibly most accurate is " the uncertainty of a future outcome". The anticipated return for some future period is known as the **expected return**. The actual return over some past period is known as the **realized return**. The simple fact that dominates investing is that

the realized return on an asset with any risk attached to it may be different from what was expected. Volatility may be described as the range of movement (or price fluctuation) from the expected level of return. The more a stock, for example, goes up and down in price, the more volatile that stock is. Because wide price swings create more uncertainty of an eventual outcome, increased volatility can be equated with increased risk. Being able to measure and determine the past volatility of a security is important in that it provides some insight into the riskiness of that security as an investment.

(ii) Standard Deviation

Investors and analysts should be at least somewhat familiar with the study of probability distributions. Since the return an investor will earn from investing is not known, it must be estimated. An investor may expect the TR (total return) on a particular security to be 10 percent for the coming year, but in truth this is only a "point estimate."

Probability Distributions: To deal with the uncertainty of returns, investors need to think explicitly about a security's distribution of probable TRs. In other words, investors need to keep in mind that, although they may expect a security to return 10 percent, for example, this is only a one-point estimate of the entire range of possibilities. Given that investors must deal with the uncertain future, a number of possible returns can, and will, occur.

In the case of a Treasury bond paying a fixed rate of interest, the interest payment will be made with, 100 percent certainty barring a financial collapse of the economy. The probability of occurrence is 1.0, because no other outcome is possible.

With the possibility of two or more outcomes, which is the norm for common stocks, each possible likely outcome must be considered and a probability of its occurrence assessed. The result of considering these outcomes and their probabilities together is a probability distribution consisting of the specification of the likely returns that may occur and the probabilities associated with these likely returns.

Probabilities represent the likelihood of various outcomes and are typically expressed as a decimal. (Sometimes fractions are used.) The sum of the

probabilities of all possible outcomes must be 1.0, because they must completely describe all the (perceived) likely occurrences.

How are these probabilities and associated outcomes obtained? In the final analysis, investing for some future period involves uncertainty, and therefore subjective estimates. Although past occurrences (frequencies) may be relied on heavily to estimate the probabilities, the past must be modified for any changes expected in the future.

Probability distributions can be either discrete or continuous. With a discrete probability distribution, a probability is assigned to each possible outcome. With a continuous probability distribution an infinite number of possible outcomes exist. The most familiar continuous distribution is the normal distribution depicted by the well-known bell-shaped curve often used in statistics. It is a two-parameter distribution in that the mean and the variance fully describe it.

To describe the single most likely outcome from a particular probability distribution, it is necessary to calculate its expected value. The expected value is the average of all possible return outcomes, where each outcome is weighted by its respective probability of occurrence. For investors, this can be described as the expected return.

We have mentioned that it's important for investors to be able to quantify and measure risk. To calculate the total risk associated with the expected return, the **variance or standard deviation** is used. This is a measure of the spread or dispersion in the probability distribution; that is, a measurement of the dispersion of a random variable around its mean. Without going into further details, just be aware that the larger this dispersion, the larger the variance or standard deviation. Since variance, volatility and risk can in this context be used synonymously, remember that the larger the standard deviation, the more uncertain the outcome.

Calculating a standard deviation using probability distributions involves making subjective estimates of the probabilities and the likely returns. However, we cannot avoid such estimates because future returns are uncertain. The prices of securities are based on investors' expectations about the future. The relevant

standard deviation in this situation is the ex ante standard deviation and not the ex post based on realized returns.

Although standard deviations based on realized returns are often used as proxies for ex ante standard deviations, investors should be careful to remember that the past cannot always be extrapolated into the future without modifications. Ex post standard deviations may be convenient, but they are subject to errors. One important point about the estimation of standard deviation is the distinction between individual securities and portfolios. Standard deviations for well-diversified portfolios are reasonably steady across time, and therefore historical calculations may be fairly reliable in projecting the future. Moving from well-diversified portfolios to individual securities, however, makes historical calculations much less reliable. Fortunately, the number one rule of portfolio management is to diversify and hold a portfolio of securities, and the standard deviations of well-diversified portfolios may be more stable.

Something very important to remember about standard deviation is that it is a measure of the **total risk** of an asset or a portfolio, including therefore **both systematic and unsystematic risk**. It captures the total variability in the asset's or portfolio's return, whatever the sources of that variability. In summary, the standard deviation of return measures the total risk of one security or the total risk of a portfolio of securities. The historical standard deviation can be calculated for individual securities or portfolios of securities using total returns for some specified period of time. This ex post value is useful in evaluating the total risk for a particular historical period and in estimating the total risk that is expected to prevail over some future period.

The standard deviation, combined with the normal distribution, can provide some useful information about the dispersion or variation in returns. In a normal distribution, the probability that a particular outcome will be above (or below) a specified value can be determined. With one standard deviation on either side of the arithmetic mean of the distribution, 68.3 percent of the outcomes will be encompassed; that is, there is a 68.3 percent probability that the actual outcome will be within one (plus or minus) standard deviation of the arithmetic mean. The probabilities are 95 and 99 percent that the actual outcome will be within two or three standard deviations, respectively, of the arithmetic mean.

(iii) Beta

Beta is a measure of the systematic risk of a security that cannot be avoided through diversification. Beta is a relative measure of risk-the risk of an individual stock relative to the market portfolio of all stocks. If the security's returns move more (less) than the market's returns as the latter changes, the security's returns have more (less) volatility (fluctuations in price) than those of the market. It is important to note that beta measures a security's volatility, or fluctuations in price, relative to a benchmark, the market portfolio of all stocks.

Securities with different slopes have different sensitivities to the returns of the market index. If the slope of this relationship for a particular security is a 45-degree angle, the beta is I.O. This means that for every one percent change in the market's return, on average this security's returns change I percent. The market portfolio has a beta of I.O. A security with a beta of 1.5, indicates that, on average, security returns are 1.5 times as volatile as market returns, both up and down. This would be considered an aggressive security because when the overall market return rises or falls 10 percent, this security, **on average**, would rise or fall 15 percent. Stocks having a beta of less than 1.0 would be considered more conservative investments than the overall market.

Beta is useful for comparing the relative systematic risk of different stocks and, in practice, is used by investors to judge a stock's riskiness. Stocks can be ranked by their betas. Because the variance of the market is a constant across all securities for a particular period, ranking stocks by beta is the same as ranking them by their absolute systematic risk. Stocks with high betas are said to be high-risk securities.

Loss Control

Any combination of actions taken to reduce the frequency or severity of losses. Installing locks, burglar or fire alarms and sprinkler systems are loss control techniques. Risk management activities that are taken to reduce the frequency and severity of losses.

Separation

It is a division of an existing loss exposure into two or more units, all used in an organization's daily operations. Separation reduces loss severity, but

may increase loss frequency because of the larger number of units exposed to loss in daily use.

Combination

It is an alliance of people or corporations for a special purpose. Combination reduces loss severity. It is a unique technique in risk management.

Transfer

Shifting the responsibility or burden for loss to another party through legislation, contract, insurance or other means. Risk transfer can also refer to shifting a physical risk or part thereof elsewhere.

Risk Retention

Every profit-making organization assumes certain business risks every day it is in operation. Many businesses have begun to realize that they can also profitably assume some of the risks that they have in the past, transferred to an insurance company. In fact, there is greater predictability with some insurance risks than most business risks encountered.

The reasons risk retention can be beneficial are:

- There is a charge for risk transfer to an insurance company, which is generally 40% to 50% more than is paid in losses, depending on the type of coverage and the amount of premium involved.
- It is inordinately expensive to document and settle relatively small losses, particularly when management time is considered.
- The collection of small losses can frequently have an adverse effect on future insurance costs.

RISKS ALREADY RETAINED

Most organizations already retain some insurance risks. For example

- They have deductibles applicable to portions of your existing property and income coverages.

- Have self-insured retention on some of their Liability coverages.
- They have no insurance coverage on various catastrophes such as flood and earthquake

RISK RETENTION LEVEL DETERMINATION

Only your executive and financial officers can determine the extent to which you should retain insurable risks and the extent to which your firm can comfortably absorb financial fluctuations in any given year. They can consider sales projections, cash flow requirements, shareholders' profit expectations, loan covenants, legal and accounting tax position, etc. All of these factors influence your ability (and willingness) to assume rather than insure given exposures to loss.

RISK RETENTION LEVEL GUIDELINES

To date, no precise formulas exist to determine a firm's proper risk retention level, but there are several guideline formulas or "rules of thumb" that have been developed. These guidelines are as follows:

[a] Accountants' Materiality Test

- A guideline used by accountants as a. measure of materiality is 5 % of net income before taxes from continuing operations.
- Based on an organization's pretax income from continuing operations of $250,000 for example, this guideline suggests they can safely retain up to $12,500 per year in unexpected losses.

[b] Net Working Capital. Method

A guideline used to determine a company's ability to quickly fund an unexpected loss, rather than its long-term financial ability to absorb loss, is 1%-5% of net working capital (The retention selected should not reduce a firm's current liability ratio below 2:1.)

Based on a hypothetical firm's financial information, this guideline could produce the following results:

Total Current Assets	$1,000,000
Total Current Liabilities	$ 500,000
Net Working Capital of	$ 500,000
Amount of risk retention	(1%) low range $5,000
	to (5%) high range $25,000

[c] New Quick Method

This guideline measures a firm's ability to cover a sudden emergency using assets that can be quickly converted to cash. It calculates current assets less inventories and current liabilities to determine a firm's "net quick" and then assumes that 1%-5% of that amount can be absorbed.

For example, based on a firm's financial information, this guideline produces the following results:

Total Current Assets		$1,000,000
Less	Inventories	$100,000
	Current Liabilities	$500,000
Net "quick"		$400,000
Amount of Risk Retention	(1%) of Low range	$4,000
	(5%) of Low range	$20,000

This method may provide an indication of the appropriate "per occurrence" retained amount.

[d] Earnings/Surplus Method

This guideline sets the annual amount of losses to be retained at a percentage (usually 1% -5%) of current earned surplus and an equal or lower percentage of the average pretax earnings for the past three to five years. This approach logically assumes that retained losses are payable from either pretax or retained earnings.

Based on the following hypothetical financial information, this guideline produces the following results:

Current Earned Surplus		$500,000
5 Year Average Pre-Tax Earnings		$250,000
TOTAL		$750,000
Amount of Risk Retention	(1%) Low Range	$7,500
	(5%) Low Range	$37,500

[e] Percentage of Sales Method

This guideline suggests a range of possible risk retention amounts equal to one-tenth of one percent to one percent of annual sales. The HIGH range is normally associated with retention capacity for the sum of all retained occurrences in one 12-month period.

For example,

Annual sales	$25,000,000
Amount of Risk Retention: • Low Range .1% • High Range 1%	25,000 250,000

[f] Earning Per Share Method

Some firms regard the impact of uninsured loss on earnings per share as a valuable guideline for determining the upper limits of annual loss retention.

A range of $.10 to $.20 per share is normally acceptable on an after-tax basis. (When dealing with earnings per share figures, you should bear in mind that a decision to retain risk rather than transfer it to an insurance company would eliminate most elements of normal premium expense, which would otherwise be charged against earnings. Therefore, it may be possible to consider higher earnings per share variances than those used here.)

By example, based on the current number of outstanding shares for a hypothetical company, this guideline produces the following results:

$.10 X 250,000 shares	= $25,000 (Low Range Retention)
$.20 X 250,000 shares	= $50,000 (High Range Retention)

RECOMMENDATIONS

- **Annual Review** - The principle single measure of a firm's loss-absorbing capacity is its revenues, its "financial bulk." When a sudden expense such as a loss occurs, expenditures are shifted, projects deferred, or finances juggled to accommodate the change. Most budgets have a certain degree of flexibility, which is one measure of the "tolerable loss level."

- **Earnings/Surplus** - In Long and Gregg's Property and Liability Handbook, Bernard Daenzer states that the minimum risk-bearing capacity "certainly should be 1% of its average annual net earnings during the last five years." "Free surplus" may be the amount of surplus available for dividends, and the figure obtained would be an annual, rather than per-loss, figure.

- **Aggregate Allowable Cost Variation** - Some finance officers establish limits within which the risk retention level may vary--say, to a maximum

of 150 percent of budgeted costs. The risk retention level should be that with the highest probability of remaining within the established limit, with the addition of total premium.

- **Materiality** - In general, 5 percent of net earnings is considered a material impact, which should be specifically footnoted in the financial statement.

The risk retention guidelines indicate that organizations can retain risk in varying amounts, and we use these guidelines to assist in determining what makes sense in different situations.

Once those levels are determined, they can be incorporated into your insurance and risk management program through the selection of individual deductibles, self-insured retention, self-insurance and/or non-insurance.

METHODS OF FINANCING RISK RETENTION -

Insurance

Risk Management is an economic operation for a company's assets, liabilities and earnings. Its objective is to minimize uncertainties and contingencies in cash flows from the impact of fortuitous losses arising in the course of the company's operations. It seeks to achieve financial stability through conscious decisions on risk retention and risk transfers. In the matter of risk transfers the decisions involve commercial contracts wherein risks are transferred contractually to vendors, contractors and suppliers or even customers. The residual risks are considered for transfer to insurer. Hence, Risk Management is an assessment of perceived risks for assets, liabilities and operations and a pursuit to keep them manageable.

Risk Management is:

- Financial protection of all fixed and current assets against fortuitous loss.
- Anticipating hazards which give rise to a loss and adoption of preventive measures
- Across all areas of assets, liabilities and operations.

- Active assessment, review and decision to retain or transfer risks.
- Financial protection for fixed costs, gross profit, alternate accommodation, increased
- Cost of working in the event of a fortuitous loss.

With increasing privatization of insurance industry it is expected it will lead to:

- Reduced premiums.
- Modern wordings and insurance practices.
- Higher standards in risk management.

Essentials of Insurance Law

The legal basis of insurance rests upon restoring an Insured to his position prior to occurrence of a loss and as agreed. The legal aspects subsisting insurance are as follows:

Insurable Interest

An Insured must be affected by a loss in terms of his assets, liabilites for damages, loss of earnings which cannot be made good, increased and continuing costs. Such interest would include vicarious liability such as a bailee or for goods held in trust.

Sum Insured

New replacement value is recommended. The issue at the time of loss of an asset is its cost of replacement. Funds required are met through internal resources or external borrowings. Insurance offers a third alternative to finance the replacement of the lost asset. In principle a similar logic pursues current assets and earnings.

Here the sum insured is lower than the actual value at the time of loss as per basis agreed then the Insured bears a rateable proportion of such loss.

Addition to above any deductible as per policy is not paid.

Indemnity

His legal principle totally eliminates any speculative loss and pays for pure loss only. It seeks to restore a person to his original position prior to loss

occurrence and excludes any profit taking and betterment through an insurance claim settlement.

Utmost Good Faith

The details and features of risks for assets and interests as insured are not entirely known or is informed to the Insurer. However ,not with standing this limitation , insurance is provided in utmost good faith of a proposal from an Insured as if made in right earnest and with due diligence.

The above reason, any material change in risk occurring during the policy period needs to be notified to the Insurer prior to the change.

Information and answers as provided within a proposal made to an Insurer constitute a legal basis for payment or rejection of a claim. They have the legal context of an implied warranty whose breach would result in repudiation of a claim.

Subrogation

Here the Insurer elects to settle a claim then the Insured's rights of recovery are to be surrendered to the Insurer at the latter's request in line with the legal principle of Indemnity.

Insurable Risks - A Balance Sheet Perspective

Liabilities	Assets
I. Net Worth	***I. Fixed & Current***
1. Business Interruption & Consequential Loss	1. Physical Loss & Damage
-Lost Profit	-Fire & Explosion
-Continuing Fixed Costs	-Storm, Flood, Earthquake
-Cost of Alternate Accommodation	-Strike, Riot, Terrorism
-Increased Cost of Working	-Malicious Damage
	-Accidental Damage

	-Breakdown
	2. Crime
	-Burglary
	-Employee Dishonesty
	-Monies
	-in transit
	-in safe
	3. Transportation Risks
	-Per Conveyance
	-Per Location
II. Liabilities for Damages	***II. Human Resources***
1. Liability to Public	1. Personal Accident
-under statute	2. Loss of Earnings
-under common law	3. Hospitalization
2. Liability arising from Products	4. Baggage
-domestic sale	5. Travel - Domestic + Overseas
-export sale	6. Director's + Officer's Liability
3. Liability as Employer	
-under Workmen Compensation Act	
-under common law	
4. Tenant's Liability	
5. Other Legal Liability	

Recommended Approach to Audit of Insurance Coverages

I. Insurance Policies:

- Review company's nature of business, property, movement, storage of products, etc.
- Verify if policies conform to set management standards and designated risk coverages.
- Examine the validity of the policy with reference to period, declarations made and premiums to be paid.
- Examine for needful inclusion of additional perils and deletion of over purchased covers.
- Check valuation for sum insured including cost of freight and erection as appropriate
- Assess and define needs for insurance in respect of expansion and new projects.
- Verify insurance adequacy for loan agreements.
- Establish satisfaction of management with reference to deductibles and cover limits.
- Any other insurance arranged for other interests and service level within the same.

II. Insurance Claims:

- Review of procedure for preparation of claim and process of submission of details to Insurer. Check for omissions to make a claim.
- Review maintenance of claims record.
- Examine for accuracy and promptness in claims as submitted.
- Examine for follow up for expeditious settlement including within it a decisive review for repair and replacement as a part of claim settlement.
- Age analysis to be done for outstanding claims for selective attention and processing.

- Review for claims lost due to being sub-standard and time barred and factor reasons into operational procedures and claims submission procedures.
- Review and factor reasons for repudiated claims into operational procedures.
- Accrual of claims and relationship issues.

REINSURANCE

An agreement whereby an insurance company transfers part or all of its risk of loss under insurance policies it writes by means of a separate contract or treaty with another insurance company. The insurance company providing the reinsurance protection is the Reinsuring Company or Re-insurer.

A contract which one insurer makes with another to protect the first insurer, wholly or partially, against loss or liability by reason of a risk under a separate and distinct contract as insurer of a third party. Reinsurance differs from coinsurance in that, in the case of reinsurance, only one insurer has a direct contractual relationship with the insured, and that insurer (commonly referred to as the "lead insurer") purchases reinsurance in order to lessen or spread the risk.

Reinsurance refers to a situation where insurance companies protect themselves against losses they may incur in the course of writing insurance business.

TYPES OF REINSURANCE

Treaty Reinsurance:

Treaty reinsurance is reinsurance of specified types or classes of insured exposures that are automatically "ceded" or accepted by the Reinsurer within the terms of the reinsurance contract or "treaty" without evaluation of each individual exposure. The reinsurance takes effect as soon as the primary insurance is sold. Treaty reinsurance is a general term used to discuss several types of coverages that can include profit sharing features.

Facultative Reinsurance:

It is reinsurance policy that provides an insurer with coverage for specific individual risks that are unusual or so large that they aren't covered in the

insurance company's reinsurance treaties. Reinsurers have no obligation to take on facultative reinsurance, but can assess each risk individually. By contrast, under treaty reinsurance, the reinsurer agrees to assume a certain percentage of entire classes of business.

Excess of Loss Reinsurance:

A form of reinsurance that, subject to a specified limit, indemnifies the reinsured for that portion of a loss (arising out of a covered occurrence under one or more original policies) that is excess of the deductible, as defined in the reinsurance contract.

Catastrophe Reinsurance:

This is a form of insurance written on an excess of loss basis in order to improve the spread of risk against unknown concentrations of liability subject to one occurrence. A deductible is chosen at the amount necessary to reduce the probable frequency of loss to an acceptable level to the reinsurer, and severity of loss to a level acceptable to the reinsured company.

Financial Reinsurance:

A specialized form of limited liability reinsurance whereby the financial and strategic motivations of the reinsured to effect the transaction take precedence over the risk transfer motivation. Also known as finite-risk reinsurance and non-traditional reinsurance.

Automatic Reinsurance:

An agreement that the insurer must cede and the reinsurer must accept all risks within certain explicitly defined limits. The reinsurer undertakes in advance to grant reinsurance to the extent specified in the agreement in every case where the ceding company accepts the application and retains its own limit.

Proportional Reinsurance:

A type of reinsurance where the ceding insurer cedes to its reinsurer a predetermined proportion of the liability and premium of those policies subject to the reinsurance agreement.

Quota Share Reinsurance:

A proportional or pro rata reinsurance treaty where the same proportion is ceded on all cessions. The reinsurer assumes a set percentage of risk for the same percentage of the premium.

Review Questions:

1. What is avoidance in risk management?
2. What is loss control?
3. Explain separation and combination concept of risk.
4. What is risk transfer?
5. What is risk retention?
6. Explain the concept of insurance.
7. Define reinsurance.

* * *

UNIT 6

SELECTING RISK MANAGEMENT TOOLS

Approaches to Selecting Risk Management Tools

One of the major challenges facing large organizations today is assessing and controlling the risks that are inherent in their daily operations. During the enactment of a business process a lot of exceptions, that is, deviations from the normal sequence of events, might occur. To assure that a process is still able to fulfill its organizational goals, process participants must be able to detect, diagnose and successfully resolve such exceptional conditions as they occur.

Traditionally, managers have relied on their experience and understanding of a process in order to handle deviations from the expected flow of events. However, the increasing complexity of modern business processes and the accelerating pace with which these processes change has made the reliance on individual managers' experience and intuition an increasingly less satisfactory way to deal with operational risks. There is an increasing need for systematic business process operational risk management methodologies. Such methodologies will assist business process designers to anticipate potential losses and instrument their processes so that losses can either be avoided or be detected in a timely way. Furthermore, when exception manifestations occur during process enactment, these methodologies assist in selecting the best way of resolving them.

Quantitative Approaches

Loss method & Expected Loss method

Generally, **Risk Management** is the process of measuring, or assessing risk and then developing strategies to manage the risk. In general, the strategies employed include transferring the risk to another party, avoiding the risk, reducing the negative effect of the risk, and accepting some or all of the consequences of a particular risk.

Traditional risk management focuses on risks stemming from physical or legal causes (e.g. natural disasters or fires, accidents, death, and lawsuits).

Financial risk management, on the other hand, focuses on risks that can be managed using traded financial instruments. Intangible risk management focuses on the risks associated with human capital, such as knowledge risk, relationship risk, and engagement-process risk. Regardless of the type of risk management, all large corporations have risk management teams and small groups and corporations practice informal, if not formal, risk management.

In ideal risk management, a prioritization process is followed whereby the risks with the greatest loss and the greatest probability of occurring are handled first, and risks with lower probability of occurrence and lower loss are handled later. In practice the process can be very difficult, and balancing between risks with a high probability of occurrence but lower loss vs. a risk with high loss but lower probability of occurrence can often be mishandled.

Intangible risk management identifies a new type of risk - a risk that has a 100% probability of occurring but is ignored by the organization due to a lack of identification ability. For example, knowledge risk occurs when deficient knowledge is applied. Relationship risk occurs when collaboration ineffectiveness occurs. Process-engagement risk occurs when operational ineffectiveness occurs. These risks directly reduce the productivity of knowledge workers, decrease cost effectiveness, profitability, service, quality, reputation, brand value, and earnings quality. Intangible risk management allows risk management to create immediate value from the identification and reduction of risks that reduce productivity.

Risk management also faces a difficulty in allocating resources properly. This is the idea of opportunity cost. Resources spent on risk management could be instead spent on more profitable activities. Again, ideal risk management spends the least amount of resources in the process while reducing the negative effects of risks as much as possible.

Worry method

Worry method is the document which is created to help clients think about potential risks, adverse consequences that could occur during the course of a project. We work with our clients to define potential risks. We then analyze these risks and define actions that can be taken to control them.

Critical probability method

Historically, three different conceptual approaches have been developed for defining probability and for determining probability values: the classical, relative frequency and subjective approaches.

In 1957, Dupont developed a project management method designed to address the challenge of shutting down chemical plants for maintenance and restarting the plants once the maintenance had been completed. Given the complexity of the process, they developed the Critical Path Method (CPM) for managing such projects. The critical path method is also called as critical probability method.

CPM provides the following benefits:

- ✓ Provides a graphical view of the project.
- ✓ Predicts the time required to complete the project.
- ✓ Shows which activities are critical to maintaining the schedule and which are not.

Steps in CPM project planning:

- ✓ Specify the individual activities.
- ✓ Determine the sequence of those activities.
- ✓ Draw a network diagram.
- ✓ Estimate the completion time for each activity.
- ✓ Identify the critical path (longest path through the network)
- ✓ Update the CPM diagram as the project progresses.

Risk Adjusted Capital Budgeting

The Capital Budgeting Process
Step 1: Identify Investment Opportunities

- How are projects initiated?
- How much is available to spend?

Step 2: Project Development
- Preliminary project review
- Technically feasible?
- Compatible with corporate strategy?

Step 3: Evaluation and Selection
- What are the costs and benefits?
- What is the project's return?
- What are the risks involved?

Step 4: Post Acquisition Control
- Is the project within budget?
- What lessons can be drawn?

Types of Projects

- Mutually Exclusive Projects: They compete in some way for a company's resources. A firm can select one or another but not both.
- Independent Projects: They do not compete with the firm's resources. A company can select one, or the other, or both.
- Expansion Projects: They will increase firm operations by producing more of the same, or else, different products.
- Replacement Projects: They will take the place of existing assets that are old, damaged, or obsolete.

Generally, **Risk Management** is the process of measuring, or assessing risk and then developing strategies to manage the risk. In general, the strategies employed include transferring the risk to another party, avoiding the risk, reducing the negative effect of the risk, and accepting some or all of the consequences of a particular risk. Traditional risk management, which is discussed here, focuses on risks stemming from physical or legal causes (e.g. natural disasters or fires, accidents, death, and lawsuits).

Financial risk management, on the other hand, focuses on risks that can be managed using traded financial instruments. Regardless of the type of risk

management, all large corporations have risk management teams and small groups and corporations practice informal, if not formal, risk management.

In ideal risk management, a prioritization process is followed whereby the risks with the greatest loss and the greatest probability of occurring are handled first, and risks with lower probability of occurrence and lower loss are handled later. In practice the process can be very difficult, and balancing between risks with a high probability of occurrence but lower loss vs. a risk with high loss but lower probability of occurrence can often be mishandled.

Risk management also faces a difficulty in allocating resources properly. This is the idea of opportunity cost. Resources spent on risk management could be instead spent on more profitable activities. Again, ideal risk management spends the least amount of resources in the process while reducing the negative effects of risks as much as possible.

The core of the risk management process is a series of five steps:

- Establish the context
- Identify risks
- Analyse risks
- Evaluate risks
- Treat risks

In parallel with the core process, communication & consultation is required to ensure adequate information is provided and conclusions are disseminated. Monitoring and review is an intrinsic part of the process required to ensure that the process is executed in a timely fashion and the identification, analysis, evaluation and treatment are kept up to date.

The standard can be found at www.standards.com.au and simple guidance on its application can be found at www.broadleaf.com.au/tutorials/Default.htm

Establish the context

Establishing the context includes planning the remainder of the process and mapping out the scope of the exercise, the identity and objectives of

stakeholders, the basis upon which risks will be evaluated and defining a framework for the process, and agenda for identification and analysis.

Identification

After establishing the context, the next step in the process of managing risk is to identify potential risks. Risks are about events that, when triggered, will cause problems. Hence, risk identification can start with the source of problems, or with the problem itself.

Source analysis

Risk sources may be internal or external to the system that is the target of risk management. Examples of risk sources are: stakeholders of a project, employees of a company or the weather over an airport.

Problem analysis

Risks are related to identified threats. For example: the threat of losing money, the threat of abuse of privacy information or the threat of accidents and casualties. The threats may exist with various entities, most important with shareholder, customers and legislative bodies such as the government.

When either source or problem is known, the events that a source may trigger or the events that can lead to a problem can be investigated. For example: stakeholders withdrawing during a project may endanger funding of the project; privacy information may be stolen by employees even within a closed network; lightning striking a B747 during takeoff may make all people onboard immediate casualties.

The chosen method of identifying risks may depend on culture, industry practice and compliance. The identification methods are formed by templates or the development of templates for identifying source, problem or event. Common risk identification methods are:

Objectives-based Risk Identification

Organizations and project teams have objectives. Any event that may endanger achieving an objective partly or completely is identified as risk.

Objective-based risk identification is at the basis of COSO's Enterprise Risk Management - Integrated Framework

Scenario-based Risk Identification

In scenario analysis different scenarios are created. The scenarios may be the alternative ways to achieve an objective, or an analysis of the interaction of forces in, for example, a market or battle. Any event that triggers an undesired scenario alternative is identified as risk.

Taxonomy-based Risk Identification

The taxonomy in taxonomy-based risk identification is a breakdown of possible risk sources. Based on the taxonomy and knowledge of best practices, a questionnaire is compiled.

Common-risk Checking

In several industries lists with known risks are available. Each risk in the list can be checked for application to a particular situation.

Assessment

Once risks have been identified, they must then be assessed as to their potential severity of loss and to the probability of occurrence. These quantities can be either simple to measure, in the case of the value of a lost building, or impossible to know for sure in the case of the probability of an unlikely event occurring. Therefore, in the assessment process it is critical to make the best educated guesses possible in order to properly prioritize the implementation of the risk management plan.

The fundamental difficulty in risk assessment is determining the rate of occurrence since statistical information is not available on all kinds of past incidents. Furthermore, evaluating the severity of the consequences (impact) is often quite difficult for immaterial assets. Asset valuation is another question that needs to be addressed. Thus, best educated opinions and available statistics are the primary sources of information. Nevertheless, risk assessment should produce such information for the management of the organisation that the

primary risks are easy to understand and that the risk management decisions may be prioritized. Thus, there have been several theories and attempts to quantify risks. Numerous different risk formulae exist, but perhaps the most widely accepted formula for risk quantification is:

Rate of occurrence multiplied by the **impact of the event** equals **risk.**

Later research has shown that the financial benefits of risk management are not so much dependent on the formulae used. The most significant factor in risk management seems to be that;

- Risk is performed frequently and
- It is done using as simple methods as possible.

In business it is imperative to be able to present the findings of risk assessments in financial terms. Robert Courtney Jr. (IBM, 1970) proposed a formulae for presenting risks in financial terms. The Courtney formulae was accepted as the official risk analysis method for the US governmental agencies. The formulae proposes calculation of ALE (Annualised Loss Expectancy) and compares the expected loss value to the security control implementation costs (cost-benefit analysis).

Potential Risk Treatments

Once risks have been identified and assessed, all techniques to manage the risk fall into one or more of these four major categories: (Dorfman, 1997)

- Transfer
- Avoidance
- Reduction (aka Mitigation)
- Acceptance (aka Retention)

Ideal use of these strategies may not be possible. Some of them may involve trade offs that are not acceptable to the organization or person making the risk management decisions.

Risk avoidance

Includes not performing an activity that could carry risk. An example would be not buying a property or business in order to not take on the liability that comes with it. Another would be not flying in order to not take the risk that the airplane were to be hijacked. Avoidance may seem the answer to all risks, but avoiding risks also means losing out on the potential gain that accepting (retaining) the risk may have allowed. Not entering a business to avoid the risk of loss also avoids the possibility of earning the profits.

Risk reduction

Involves methods that reduce the severity of the loss. Examples include sprinklers designed to put out a fire to reduce the risk of loss by fire. This method may cause a greater loss by water damage and therefore may not be suitable. Halon fire suppression systems may mitigate that risk, but the cost may be prohibitive as a strategy.

Modern software development methodologies reduce risk by developing and delivering software incrementally. Early methodologies suffered from the fact that they only delivered software in the final phase of development; any problems encountered in earlier phases meant costly rework and often jeopardized the whole project. By developing in increments, software projects can limit effort wasted to a single increment. A current trend in software development, spearheaded by the Extreme Programming community, is to reduce the size of increments to the smallest size possible, sometimes as little as one week is allocated to an increment.

Risk retention

Involves accepting the loss when it occurs. True self insurance falls in this category. Risk retention is a viable strategy for small risks where the cost of insuring against the risk would be greater over time than the total losses sustained. All risks that are not avoided or transferred are retained by default. This includes risks that are so large or catastrophic that they either cannot be insured against or the premiums would be infeasible. War is an example since most property and risks are not insured against war, so the loss attributed by war is retained by the insured. Also any amounts of potential loss (risk) over the

amount insured is retained risk. This may also be acceptable if the chance of a very large loss is small or if the cost to insure for greater coverage amounts is so great it would hinder the goals of the organization too much.

Risk transfer

Means causing another party to accept the risk, typically by contract or by hedging. Insurance is one type of risk transfer that uses contracts. Other times it may involve contract language that transfers a risk to another party without the payment of an insurance premium. Liability among construction or other contractors is very often transferred this way. On the other hand, taking offsetting positions in derivatives is typically how firms use hedging to financially manage risk.

Some ways of managing risk fall into multiple categories. Risk retention pools are technically retaining the risk for the group, but spreading it over the whole group involves transfer among individual members of the group. This is different from traditional insurance, in that no premium is exchanged between members of the group up front, but instead losses are assessed to all members of the group.

Create the Plan

Decide on the combination of methods to be used for each risk. Each risk management decision should be recorded and approved by the appropriate level of management. For example, a risk concerning the imago of the organisation should have top management decision behind it whereas IT management would have the authority to decide on computer virus risks.

The risk management plan should propose applicable and effective security controls for managing the risks. For example, an observed high risk of computer viruses could be mitigated by acquiring and implementing anti virus software. A good risk management plan should contain a schedule for control implementation and responsibile persons for those actions.

Implementation

Follow all of the planned methods for mitigating the effect of the risks. Purchase insurance policies for the risks that have been decided to be transferred to an insurer, avoid all risks that can be avoided without sacrificing the entity's goals, reduce others, and retain the rest.

Review and evaluation of the plan

Initial risk management plans will never be perfect. Practice, experience, and actual loss results, will necessitate changes in the plan and contribute information to allow possible different decisions to be made in dealing with the risks being faced.

Risk analysis results and management plans should be updated periodically. There are two primary reasons for this: 1.) to evaluate whether the previously selected security controls are still applicable and effective and 2.) to evaluate the possible risk level changes in the business environment. For example, information risks are a good example of rapidly changing business environment.

If risks are improperly assessed and prioritized, time can be wasted in dealing with risk of losses that are not likely to occur. Spending too much time assessing and managing unlikely risks can divert resources that could be used more profitably. Unlikely events do occur, but if the risk is unlikely enough to occur, it may be better to simply retain the risk, and deal with the result if the loss does in fact occur.

Prioritizing too highly the Risk management processes itself could potentially keep an crganization from ever completing a project or even getting started. This is especially true if other work is suspended until the risk management process is considered complete.

It is also important to keep in mind the distinction between risk and uncertainty.

Enterprise Risk Management

In Enterprise Risk Management, a risk is defined as a possible event or circumstance that can have negative influences on the Enterprise in question. Its impact can be on the very existance, the resources (human and capital), the products and services, or the customers of the Enterprise, as well as external impacts on Society, Markets or the Environment.

Project Management

In project management, a risk is more narrowly defined as a possible event or circumstance that can have negative influences on a project. Its influence can be on the schedule, the resources, the scope and/or the quality.

In project management parlance, when a risk escalates, it becomes a liability. A liability is a negative event or circumstance that is hindering the project.

Some of the processes for assessing risk include the following (the parentheses contain some of the jargon used to refer to them).

- Choosing unique identifiers for referring to the same risk in company or project documents (identification).
- Describing the risk and how it could become a liability (description).
- Assessing the consequences of that (effect).
- Considering what precautions could be taken to prevent it (precaution).
- Drawing up contingency plans or procedures for handling it (contingency).
- Categorizing the risk as new, ongoing or closed (risk status)
- Estimating the probability of the risk becoming a liability (Risk escalation probability, P)
- Estimating the consequences in terms of time for the project (Schedule impact, S)

In addition, every probable risk can have a pre-formulated plan to deal with it to deal with its possible consequences (to ensure contingency if the risk becomes a liability).

From the information above and the average cost per employee over time, or Cost Accrual Ratio, a project manager can estimate.

The cost associated with the risk if it arises, estimated by multiplying employee costs per unit time by the estimated time lost (cost impact, C where C = Cost Accrual Ratio * S)

The probable increase in time associated with a risk (schedule variance due to risk, Rs where Rs = P * S):

Sorting on this value puts the highest risks to the schedule first. This is intended to cause the greatest risks to the project to be attempted first so that risk is minimized as quickly as possible.

This is slightly misleading as schedule variances with a large P and small S and vice versa are not equivalent. (The risk of the RMS Titanic sinking vs. the passengers' meals being served at slightly the wrong time).

The probable increase in cost associated with a risk (cost variance due to risk, Rc where Rc = P*C = P*CAR*S = P*S*CAR)

Sorting on this value puts the highest risks to the budget first.

See concerns about schedule variance as this is a function of it, as illustrated in the equation above.

Risk in a project or process can be due either to special causes of deviation or common causes of deviation and requires appropriate treatment. That is to re-iterate the concern about extremal cases not being equivalent in the list immediately above.

Risk management activities as applied to project management

In project management, risk management includes the following activities:

- Planning how risk management will be held in the particular project. Plan should include risk management tasks, responsibilities, activities and budget.

- Assigning risk officer - a team member other than a project manager who is responsible for foreseeing potential project problems. Typical characteristic of risk officer is a healthy skepticism.

Maintaining live project risk database. Each risk should have the following attributes: opening date, title, short description, probability and importance. Optionally risk can have assigned person responsible for its resolution and date till then risk still can be resolved.

Creating anonymous risk reporting channel. Each team member should have possibility to report risk that he foresees in the project.

Preparing mitigation plans for risks that are chosen to be mitigated. The purpose of the mitigation plan is to describe how this particular risk will be handled – what, when, by who and how will be done to avoid it or minimize consequences if it becomes a liability.

Summarizing planned and faced risks, effectiveness of mitigation activities and effort spend for the risk management.

Risk management is simply a practice of systematically selecting cost effective approaches for minimising the effect of threat realisation to the organisation. All risks can never be fully avoided or mitigated simply because of financial and practical limitations of the real world. Therefore all organisations have to accept some level of residual risks which still may realise despite their efforts.

Whereas risk management tends to be pre-emptive, Business Continuity Planning (BCP) was invented to deal with the consequences of realised residual risks. The necessity to have BCP in place raises because even very unlikely events will occur if a necessarily long time is available. Risk managment and BCP are often mistakenly seen as rivals or overlapping practices. In fact these processes are so tightly tied together that such separation seems artificial. For example, the risk management process creates important inputs for the BCP

(assets, impact assessments, cost estimates etc). Risk management also proposes applicable controls for the observed risks. Therefore, risk management covers several areas that are vital for the BCP process. However, the BCP process goes beyond risk management's pre-emptive approach and moves on from the assumption that the disaster will realise at some point.

Review questions:

1. List out some risk management tools.
2. Explain different quantitative approaches for risk management.
3. What is critical probability method?
4. What is capital budgeting?
5. What is enterprise risk management?

* * *

MODEL QUESTION PAPER

Paper 3.3 PROJECT RISK MANAGEMENT

Time: 3 Hours Max. Marks: 100

SECTION - A (5 x 8 = 40)

Answer any Five questions

All questions carry equal marks

1. Define risk management and its objectives.
2. Explain the risk management process.
3. Describe the role of risk management in different types of business.
4. Explain the risk identification methods.
5. Describe the risk measurement methods.
6. What are the civil liabilities of business houses?
7. List out and explain any three risk management techniques.
8. Explain the steps in critical probability method.

SECTION - B (4 x 15 = 60)

Answer any **Four** questions

9. Explain in detail the classification of risk.
10. Describe the contribution of risk management to business and society.
11. Explain the financial statement analysis in risk management.
12. Explain different types of loss exposures.
13. Explain the concept and need for risk retention.
14. Describe the insurance and reinsurance concepts in risk management.
15. Explain the risk adjusted capital budgeting technique.

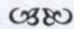
LIST OF REFERENCE BOOKS

1. Arthur Williams C, Richard M Heins, Risk Management and Insurance, McGraw Hill publications.

2. Ahearn J L and Pritehett S T, Risk Insurance, West Publishing Co.,

3. Lalley P Edward, Corporate Uncertainty and Risk Management, New York Risk Management Society Publication.

4. Insurance Institute of India : Study materials.



Educate ⇗ Empower ⇗ Elevate

Alagappa University formed in 1985 has emerged from the galaxy of institutions initially founded by the munificent and multifaceted personality, Dr. RM. Alagappa Chettiar in his home town at Karaikudi. Groomed to prominence as yet another academic constellation in Tamil Nadu, it is located in a sprawling and ideally suited expanse of about 420 acres in Karaikudi.

Alagappa University was established in 1985 under an Act of the State Legislature. The University is recognised under Sec. 2(f) and Sec.12(B) of the University Grants Commission. It is a member of the Association of Commonwealth Universities and the Association of Indian Universities. The University is accredited with 'A' Grade by NAAC.

The Directorate of Distance Education offers various innovative, job-oriented and socially relevant academic programmes in the field of Arts, Science, IT, Education and Management at the graduate and post-graduate levels. It has an excellent network of Study Centres throughout the country for providing effective service to the student community.

The distance education programmes are also offered in South-East Asian countries such as Singapore and Malaysia; in Middle-East countries, viz., Bahrain, Qatar, Dubai; and also at Nepal and Sri Lanka. The programmes are well received in India and abroad.



ALAGAPPA UNIVERSITY
(Accredited with 'A' Grade by NAAC)
Karaikudi 630 003

DIRECTORATE OF DISTANCE EDUCATION
(Recognized by Distance Education Council (DEC), New Delhi)